Základy matematiky

Pavel Řehák

(verze 13. prosince 2011)

Pár slov na úvod

Tento text tvoří doplněk k předmětu Základy matematiky, který je nyní již pevnou součástí výuky v podzimním semestru (pro Pedagogické asistenství matematiky pro ZŠ). Poprvé byl předmět v této formě realizován na podzim r. 2008 jako reakce na vzrůstající potřebu položení pevných a jasných základů matematiky, nezbytných pro další studium.

Poněvadž je tento text doplňkem, nevyčerpává vše, co se na přednáškách probírá. Ovšem snaží se alespoň ve stručnosti zachytit nejdůležitější pojmy a fakta. V kombinaci s poznámkami z přednášek (kde zejména podrobněji komentujeme probíranou látku, doplňujeme ji, uvádíme ilustrativní příklady a diskutujeme) a s materiálem ze cvičení by měl tvořit postačující zdroje k přípravě na zkoušku. Je samozřejmě vítána i samostatná iniciativa studentů, kdy sami čerpají i z jiných zdrojů (a těch je skutečně nepřeberné množství). Proto (a nejen proto) je každá kapitola zakončena odkazy na další vhodnou literaturu včetně případných komentářů.

Text byl průběžně vytvářen zejména během první výuky předmětu v semestru podzim 2008 a posléze byl několikrát aktualizován. Je třeba upozornit na to, že již jednou vytvořené partie mohou (a s velkou pravděpodobností budou) doznávat určitých změn i v pozdější době – v zájmu zkvalitnění textu.

Obsahem tohoto kurzu jsou mimo jiné i velmi důležité partie matematiky, které svým způsobem tvoří její základní kameny (např. logika a teorie množin). O těchto teoriích lze napsat desítky knih. Nám však jde v této fázi spíše o nalezení vhodného a dostatečně přesného matematického jazyka, který bude nezbytný pro potřeby dalšího studia i pro potřeby praxe. Vybrali jsme proto pouze to „nejzákladnější“, přičemž náš přístup bude velmi často neformální (intuitivní). Členění textu je rovněž spíše přizpůsobeno našim potřebám.

Nově zaváděné a důležité pojmy budou zpravidla vynačeny *kurzívou.*

Budu vděčný každému, kdo mne upozorní na nepřesnosti či chyby v textu (některé nepřesnosti – či spíše zjednodušení – jsou ovšem „záměrné“ vzhledem k výše popsanému přístupu).

Brno, 13. prosince 2011, Pavel Řehák

Obsah

Kapitola 1

Základní pojmy matematické logiky

Náš přístup k výrokové a predikátové logice bude intuitivní (neformální).

1.1 Výroky, logické spojky, složené výroky, výrokové formule

Výrokem rozumíme jakékoliv tvrzení (intuitivně řečeno oznamovací větu), které je dostatečně smysluplné, aby bylo možno říci, že je pravdivé nebo nepravdivé.

Poznámka 1.1. (i) Nemusíme být schopni o pravdivosti rozhodnout. Např. „Český kníže Bořivoj měl 1.1. 880 rýmu.“ je výrok.

(ii) Pravdivým výrokům je zvykem přiřazovat *pravdivostní hodnotu* 1, nepravdivým hodnotu 0.

(iii) Náš popis výroku není přesná definice. Je to pouhé vymezení. Axiomatický přístup je „přesnější“.

Příklad 1.1. „Prší.“ je výrok. „Prší?“ není výrok. „Kéž by pršelo!“ není výrok. „Číslo x je sudé.“ není výrok.

Pro snazší vyjadřování budeme používat *výrokové proměnné* $A, B, \ldots,$ které zastupují výroky.

Z výroků lze vytvářet výroky složitější (tzv. *složené výroky*). K jejich vytváření se užívají *logické spojky.* Nechť A, B jsou výroky. Potom definujeme

- *Negace* výroku A (značíme $\neg A$): Výrok, který je pravdivý, právě když A je nepravdivý.
- *Konjunkce* výroků A, B (značíme $A \wedge B$): Výrok, který je pravdivý, právě když A, B jsou oba (zároveň) pravdivé.
- *Disjunkce* výroků A, B (značíme $A \vee B$): Výrok, který je pravdivý, právě když alespoň jeden z výroků A, B je pravdivý.
- *Implikace* výroku B výrokem A (značíme $A \Rightarrow B$): Výrok, který je pravdivý, právě když nenastává případ, že A je pravdivý a zároveň B je nepravdivý.
- *Ekvivalence* výroků A, B (značíme $A \Leftrightarrow B$): Výrok, který je pravdivý, právě když A, B jsou oba zároveň pravdivé, anebo oba zároveň nepravdivé.

Výrokovou formulí rozumíme výraz vytvořený z konečného počtu výrokových proměnných, logických spojek a popřípadě závorek. (Často se v literatuře (přesněji) definuje tento pojem rekurzí).

Častým způsobem výpočtu pravdivostních hodnot dané formule (v závislosti na pravdivostních hodnotách proměnných, které se v ní vyskytují) jsou tabulky *pravdivostních hodnot*.

Tautologií nazýváme výrokovou formuli, jejíž pravdivostní hodnota je 1 při každém ohodnocení výrokových proměnných, které se v ní vyskytují.

Kontradikcí nazýváme výrokovou formuli, jejíž pravdivostní hodnota je 0 při každém ohodnocení výrokových proměnných, které se v ní vyskytují.

1.2 Výrokové formy, kvantifikátory, kvantifikované výroky

Jestliže se nějaké tvrzení (obsahující jednu nebo více proměnných) stane výrokem, dosadíme-li za proměnné konkrétní hodnoty (konstanty z oboru proměnných), nazýváme takové tvrzení *výrokovou formou*. Značíme $V(x)$ výrokovou formu o jedné proměnné a $V(x_1, \dots, x_n)$ výrokovou formu o n proměnných.

Pomocí logických spojek lze pak vytvářet *složené výrokové formy*.

Dosazení konstant za proměnné do výrokové formy není jediným způsobem, jak z ní vytvořit výroky. Další (významnou) možností je tzv. *kvantifikace*. Provádíme ji pomocí jistých slovních spojení zvaných *kvantifikátory*:

- Obecný kvantifikátor (značíme $\forall$). Jazykový význam: „pro každé“.
- Existenční kvantifikátor (značíme $\exists$). Jazykový význam: „existuje (alespoň jedno)“.
- Kvantifikátor jednoznačné existence (značíme $\exists!$). Jazykový význam: „existuje právě jedno“.

Nechť $V(x)$ je výroková forma proměnné x. Pak pomocí těchto kvantifikátorů lze vytvořit následující typy základních *kvantifikovaných výroků*:

- $\forall x \in M : V(x)$ (čteme: „Pro každé $x \in M$ platí $V(x)$.“)
- $\exists x \in M : V(x)$ (čteme: „Existuje (alespoň jedno) $x \in M$, pro které platí $V(x)$.“)
- $\exists! x \in M : V(x)$ (čteme: „Existuje právě jedno $x \in M$, pro které platí $V(x)$.“)

Chceme-li tvořit výroky pomocí kvantifikátorů z výrokové formy více proměnných, musíme přiřadit kvantifikátor každé proměnné.

1.3 Negování výroků

Negaci výroku lze získat předřazením slov „Není pravda, že … “. Zpravidla však užíváme gramaticky vhodnějších tvarů a následujících postupů:

(i) Při negování jednoduchých nekvantifikovaných výroků používáme dva způsoby (uvažujme např. výrok „Číslo 3 je kladné“): záměna „je“ za „není“ („Číslo 3 není kladné“) nebo připojení předpony ne- („Číslo 3 je nekladné“).

(ii) Při negování složených nekvantifikovaných výroků postupujeme často podle tabulky

složený výrok	negace
$A \wedge B$	$\neg A \vee \neg B$
$A \vee B$	$\neg A \wedge \neg B$
$A \Rightarrow B$	$A \wedge \neg B$
$A \Leftrightarrow B$	$(A \wedge \neg B) \vee (\neg A \wedge B)$

Zkuste si promyslet, proč volíme zrovna tyto způsoby negace.

(iii) Negaci jednoduchých nekvantifikovaných výroků provádíme záměnou kvantifikátorů a negací výrokové formy (např. negací výroku $\forall x \in M : V(x)$ je výrok $\exists x \in M : \neg V(x)$). Totéž pravidlo používáme u kvantifikovaných výroků vytvořených z výrokové formy o více proměnných.

(iv) Negování složených kvantifikovaných výroků provádíme kombinací pravidel uvedených ve (ii) a (iii).

1.4 Literatura

Existuje velmi mnoho literatury, ze které lze čerpat (od skript po odborné monografie). Přístupy se mohou velmi lišit (od neformálních po formální, od „méně přesných“ po precizní). Jak již bylo řečeno na začátku, pro naše potřeby základního kurzu jsme zvolili poněkud jednodušší (neformální) přístup, který nám však prozatím bohatě postačuje (v našem případě mohou být – po jistém rozšíření obsahu – vhodnými zdroji např. [1,4,5]; zde se má na mysli ne pouze náš text, ale i obsah přednášek). Nakonec si dovolím upozornit na vynikající knihu [6].

[1] I. Bušek, E. Calda, Matematika pro gymnázia. Základní poznatky z matematiky (3. vydání), Prometheus, Praha 2006.

[2] K. Devlin, Jazyk matematiky, Argo, Dokořán, Praha 2002.

[3] E. Fuchs, Teorie množin pro učitele, Masarykova univerzita, Brno 1999.

[4] J. Kuben, P. Šarmanová, Diferenciální počet funkcí jedné proměnné, VŠB TU Ostrava 2006.

[5] J. Polák, Přehled středoškolské matematiky (7. vydání), Prometheus, Praha 2000.

[6] A. Sochor, Logika pro všechny ochotné myslet, Karolinum (v přípravě).

[7] R. Thiele, Matematické důkazy, SNTL, Praha 1986.

Kapitola 2

Matematické důkazy

2.1 Tvary matematických vět

Matematické věty se objevují zpravidla v nějakém z následujících tvarů.

(i) Tzv. *obecná věta* „$\forall x \in M : V(x)$“. Případně můžeme uvažovat prostě větu typu „Platí V“.

(ii) Tzv. *existenční věta* „$\exists x \in M : V(x)$“ nebo věta o jednoznačné existenci „$\exists! x \in M : V(x)$“.

(iii) Velmi často má obecná věta tvar implikace „$\forall x \in M : A(x) \Rightarrow B(x)$“ (nebo stručně „$A(x) \Rightarrow B(x)$“, případně „$A \Rightarrow B$“). A se nazývá *předpoklad věty*, B se nazývá *tvrzení věty*. A se nazývá *postačující* (nebo *dostatečná*) *podmínka* pro B. B se nazývá *nutná podmínka* pro A.

(iv) Má-li věta tvar ekvivalence „$A \Leftrightarrow B$“, často ji lze chápat (dokazovat) jako dvě věty typu (iii), neboť platí $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$. Někdy mívají matematické věty také tento tvar: „Jestliže platí výrok P, pak výroky $A_1, \dots, A_n$ ($n \geq 2$) jsou ekvivalentní“. Potom stačí dokazovat $A_1 \Rightarrow A_2$, $A_2 \Rightarrow A_3$, …, $A_{n-1} \Rightarrow A_n$, $A_n \Rightarrow A_1$ (pořadí není podstatné; důležité je, aby se kruh implikací uzavřel).

2.2 Důkaz přímý, důkaz nepřímý, důkaz sporem

(i) *Přímý důkaz* implikace $A \Rightarrow B$ spočívá v tom, že sestavíme řetězec platných implikací $A \Rightarrow A_1$, $A_1 \Rightarrow A_2$, …, $A_n \Rightarrow B$. Při řešení úlohy typu „Dokažte výrok V.“, kde „začátek řetězce“ není znám (ale i v případě dokazování implikací), můžeme pomocí jistého rozboru (souvisí s hledáním myšlenky důkazu) hledat nějaký možný začátek řetězce, kdy vyjdeme od hledaného (tedy od tvrzení) a pomocí řetězce úsudků dojdeme k nějakému výroku, jehož pravdivost je nám známa (případně, dokazujeme-li implikaci, dojdeme k danému, tedy k předpokladu). Důkaz výroku V se pak pokusíme sestrojit jako řetězec obrácených implikací.

(ii) *Nepřímý důkaz* implikace $A \Rightarrow B$ je založen na vztahu $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$. Tj., přímo dokazujeme implikaci $\neg B \Rightarrow \neg A$.

(iii) *Důkaz sporem* implikace $A \Rightarrow B$ je založen na vztahu $(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$. (Sporem) předpokládáme současnou platnost A a $\neg B$ a řadou platných implikací pak odvodíme spor s některým z předpokladů nebo jiným výrokem (spor je stav, kdy pro nějakou formuli C ukážeme, že současně platí C a $\neg C$).

2.3 Důkazy existence, neexistence a jednoznačnosti

Existenční důkazy lze vést přímo či nepřímo.

Přímý důkaz je buď *ryze existenční* (tj. existence objektu se přímo dokáže bez jeho určení; např. pomocí nějakého existenčního principu (Dirichletův princip, princip spojitosti apod.)) nebo je *konstrukční* (objekt se sestrojí).

Při nepřímém důkazu vyvozujeme spor z předpokladu, že objekt neexistuje. Podobně jako v případě ryze existenčního přímého důkazu sice nepřímý důkaz zaručí řešitelnost z hlediska logiky, nedává však zpravidla žádné pokyny, jak toto řešení sestrojit.

Při *důkazu neexistence* postupujeme velmi často sporem.

Při *důkazech jednoznačnosti* zpravidla ukazujeme, že existuje alespoň jeden objekt a současně existuje nejvýše jeden objekt (zde velmi často postupujeme sporem; přepokládáme existenci dvou různých objektů, pro které výrok platí).

K této i předchozí podkapitole poznamenejme, že obecný výrok nebo existenční tvrzení lze vyvrátit již jediným příkladem, tzv. *protipříkladem.*

2.4 Důkazy matematickou indukcí

Používáme pro důkazy vět typu

$$„\forall n \in M = \{n_0, n_0+1, n_0+2, \dots\} \subset \mathbb{Z} : V(n).“$$

(velmi často $M = \mathbb{N}$).

Důkaz je založen na následujícím *principu matematické* (neboli *úplné*) *indukce*:

Nechť výroková forma $V(n)$ je definována pro každé $n \in M$. Dále nechť

(I) $V(n_0)$ je platný výrok.

(II) $\forall n \in M$: $V(n)$ je platný výrok $\Rightarrow V(n+1)$ je platný výrok.

Potom $V(n)$ platí pro každé $n \in M$.

Poznámka 2.1. (i) Podmínka (II) je tzv. *indukční krok*, $V(n)$ se v tomto kroku nazývá *indukční předpoklad*.

(ii) Důkaz matematickou indukcí se tedy skládá ze dvou kroků: (I) Důkaz platnosti tvrzení $V(n_0)$. (II) Důkaz indukčního kroku.

(iii) Lze nalézt i jiné formulace principu matematické indukce. Např. v podmínce (II) můžeme mít $V(n_0), V(n_0+1), \dots, V(n) \Rightarrow V(n+1)$. Tento předpoklad je silnější než v původním principu. Teoreticky jsou ale oba principy ekvivalentní. V praxi se však vyskytují problémy, které se mnohem snáze řeší pomocí této modifikace.

(iv) Pomocí indukce nejenom dokazujeme tvrzení, ale též konstruujeme objekty, či definujeme.

2.5 Literatura

[1] I. Bušek, E. Calda, Matematika pro gymnázia. Základní poznatky z matematiky (3. vydání), Prometheus, Praha 2006.

[2] K. Devlin, Jazyk matematiky, Argo, Dokořán, Praha 2002.

[3] J. Polák, Přehled středoškolské matematiky (7. vydání), Prometheus, Praha 2000.

[4] O. Odvárko, E. Calda, J. Šedivý, S. Židek, Metody řešení matematických úloh, SPN, Praha 1990.

[5] R. Thiele, Matematické důkazy, SNTL, Praha 1986.

Kapitola 3

Základy teorie množin

Upozorňujeme, že v této partii (jako ostatně i v jiných partiích) se mohou v různé literatuře přístupy k zavádění jednotlivých základních pojmů více či méně lišit.

3.1 Základní pojmy

Množinou rozumíme soubor (souhrn) navzájem různých (rozlišitelných) (matematických či jiných) objektů. O každém objektu musí být možné rozhodnout, zda do dané množiny patří, či nikoliv. Jednotlivé objekty, které patří do dané množiny, se nazývají *prvky* množiny.

Množiny obvykle (ovšem ne vždy) značíme velkými písmeny a prvky malými písmeny. Pozor: množiny mohou někdy vystupovat jako prvky jiných množin.

Zápis $a \in A$ znamená, že *a je prvkem množiny A*. Zápis $a \notin A$ znamená, že *a není prvkem množiny A*.

Množina je jednoznačně určena svými prvky. Proto dvě množiny, nezávisle na způsobu jejich zadání, považujeme za stejné, právě když mají stejné prvky (tzv. *extenzionalita*). Můžeme tedy psát $A = B \Leftrightarrow (\forall x : x \in A \Leftrightarrow x \in B)$.

Existuje tzv. *prázdná množina*, která se vyznačuje tím, že nemá žádné prvky. Označujeme ji symbolem $\emptyset$.

Množina, která má konečný počet prvků (tj. buď je prázdná, anebo počet jejich prvků je dán přirozeným číslem), se nazývá *konečná množina*. Počet prvků konečné množiny A označujeme symbolem $|A|$ (později, kdy jistým způsobem rozšíříme pojem počtu prvků, budeme spíše používat označení card A.) Každá množina, která není konečná, se nazývá *nekonečná množina*.

Množinu lze zadat různými způsoby, nejčastěji *výčtem prvků* nebo *charakteristickou vlastností*. Poznamenejme, že z extenzionality vyplývá např. $\{a, b\} = \{b, a\}$. Dále platí např. $\{x, x, y\} = \{x, y\}$.

Poznámka 3.1. Pojem množiny zde zavedený je pouze intuitivní a byl v podobném tvaru (ale též intuitivně) zaveden G. Cantorem v r. 1872. V pozdější době se však ukázalo, že toto pojetí množiny je nevyhovující. Byly totiž objeveny tzv. antinomie, neboli paradoxy, které ukazují její spornost. Jedním z nejznámějších paradoxů je tzv. *Russelův paradox*: Připusťme existenci množiny $A = \{X : X \text{ je množina}, X \notin X\}$. Z definice množiny A potom vyplývá, že nemůže platit ani vztah $A \in A$ (odtud totiž plyne $A \notin A$), ani vztah $A \notin A$ (odtud zase naopak plyne $A \in A$). Tyto paradoxy byly později odstraněny tím, že teorie množin byla vybudována axiomaticky. Tato axiomatická teorie však překračuje rámec naší učební látky.

Na základě této poznámky vidíme, že je potřeba opatrnosti při uvažování jakýchsi „univerzálních souborů“ jako „souboru všech množin“ apod. Tyto soubory nemohou být množinami.

3.2 Základní množinové vztahy a operace

O *rovnosti* množin A, B (tj. $A = B$) jsme se zmínili již výše.

Říkáme, že množina A je *podmnožina* množiny B a píšeme $A \subseteq B$, právě když $\forall x : x \in A \Rightarrow x \in B$. Vztah $\subseteq$ se nazývá *množinová inkluze*. Jestliže $A \subseteq B$ a $A \neq B$, pak říkáme, že A je *vlastní podmnožina* množiny B a píšeme $A \subset B$. Jestliže A není podmnožina množiny B, píšeme $A \not\subseteq B$.

Pro libovolné množiny A, B, C zřejmě platí $A \subseteq A$, $\emptyset \subseteq A$, $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$, $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$. Poslední vztah je velmi užitečný při dokazování množinových rovností.

Jsou-li A, B množiny, pak můžeme utvořit další množiny

$$A \cup B = \{x : x \in A \vee x \in B\},$$
$$A \cap B = \{x : x \in A \wedge x \in B\},$$
$$A \setminus B = \{x : x \in A \wedge x \notin B\},$$

které postupně nazýváme *sjednocení, průnik a rozdíl* množin A a B. Později budeme tyto operace zavádět i na systémech množin.

Platí řada důležitých vztahů (dokažte si je), např.:

$$
\begin{aligned}
A \cup B &= B \cup A \quad \text{(komutativní zákon)}\\
A \cap B &= B \cap A \quad \text{(komutativní zákon)}\\
(A \cup B) \cup C &= A \cup (B \cup C) \quad \text{(asociativní zákon)}\\
(A \cap B) \cap C &= A \cap (B \cap C) \quad \text{(asociativní zákon)}\\
A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C) \quad \text{(de Morganův zákon)}\\
A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C) \quad \text{(de Morganův zákon)}
\end{aligned}
$$

Dále je užitečné si uvědomit následující vztahy (promyslete si, proč platí):

$$
\begin{aligned}
x \notin A \cup B &\Leftrightarrow (x \notin A \wedge x \notin B)\\
x \notin A \cap B &\Leftrightarrow (x \notin A \vee x \notin B)\\
x \notin A \setminus B &\Leftrightarrow (x \notin A \vee x \in B)
\end{aligned}
$$

Pro libovolnou množinu A definujeme *systém všech podmnožin množiny* A a označujeme jej 2^A (případně $\mathcal{P}(A)$), tedy $2^A = \{X : X \subseteq A\}$. Jestliže $|A| = n$, potom $|2^A| = 2^n$.

Množiny a vztahy mezi nimi lze znázorňovat graficky pomocí tzv. *Vennových diagramů*.

Důkazy množinových rovností a dalších vztahů lze provádět více způsoby (ne všechny jsou však vždy zcela vhodné či korektní):

- *Princip neurčitého prvku:* Při důkazu vztahu $A \subseteq B$ vezmeme pevný, ale libovolný prvek $x \in A$ a ukážeme, že $x \in B$.
- *Tabulková metoda:* Do tabulky vypisujeme všechny možné kombinace (skupiny) – třídíme prvky podle jejich vztahu ke vstupním množinám (1 pro „je prvkem“, 0 pro „není prvkem“). V dalších sloupcích pak postupně přidáváme další potřebné operace dle zadání. Používáme v podstatě podobný přístup jako u pravdivostních tabulek ve výrokovém počtu.
- *Obrázková metoda:* Založena na použití Vennových diagramů. Zde v podstatě nejde o korektní důkaz (metoda je totiž vázána na jednu konkrétní reprezentaci množin pomocí určitých geometrických útvarů). Nicméně Vennovy diagramy velmi dobře slouží pro získání přehledu o situaci a pro odhad toho, jaký výsledek můžeme očekávat. Dále jsou velmi užitečné (a korektní) pro důkaz toho, že nějaký vztah neplatí – nalezení vhodného konkrétního příkladu.

3.3 (Ne)uspořádané dvojice a kartézský součin

Neuspořádanou dvojicí prvků a, b rozumíme množinu $\{a, b\}$ (nezáleží na pořadí, tj. vždy platí $\{a, b\} = \{b, a\}$). Podobně definujeme neuspořádanou n-tici prvků $x_1, \ldots, x_n$ ($n \in \mathbb{N}, n \geq 2$) jako $\{x_1, \ldots, x_n\}$.

Chceme-li uvažovat tzv. uspořádanou dvojici (a, b) (tj. dvojici, kde záleží na pořadí) je přirozené požadovat platnost vztahu $(a, b) = (c, d)$, právě když $a = c$ a zároveň $b = d$. Lze ukázat, že uspořádaná dvojice definovaná následujícím způsobem má požadovanou vlastnost. Mějme dány dva prvky a, b, přičemž nevylučujeme případ $a = b$. *Uspořádanou dvojici* (a, b) definujeme jako $(a, b) = \{\{a\}, \{a, b\}\}$. Je lehké vidět, že $(a, a) = \{\{a\}\}$. Uspořádanou n-tici definujeme indukcí takto: $(a) = \{a\}$, $(a_1, \ldots, a_n) = (a_1, (a_2, \ldots, a_n))$. Lze opět ukázat, že $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$, právě když $a_1 = b_1, \ldots, a_n = b_n$.

Jestliže A, B jsou libovolné množiny, pak množina $A \times B = \{(x, y) : x \in A, x \in B\}$ se nazývá *kartézský součin množin* A, B (v tomto pořadí). Analogicky definujeme $A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i, i = 1, \ldots, n\}$. Pro počet prvků (v případě konečných množin A, B) platí $|A \times B| = |A| \cdot |B|$.

Zde jsou některé vztahy pro sjednocení, průnik, rozdíl a kartézský součin (dokažte si je):

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$
$$A \times (B \setminus C) = (A \times B) \setminus (A \times C)$$

3.4 Literatura

Jak již bylo řečeno na začátku, mohou se v různé literatuře přístupy k základním pojmům více či méně lišit. Upozorňujeme, že monografie [1] je již jistým způsobem pokročilá a je určena pouze pro vážné zájemce o problematiku. Rovněž skripta [4] se budou hodit spíše v pokročilejším kurzu teorie množin v některém z dalších semestrů. Pro naše potřeby jsou nyní nejvhodnějšími zdroji [2,5,6,8].

[1] B. Balcar, P. Štěpánek, Teorie množin, Academia, Praha 1986.

[2] J. Bečvář a kol., Seznamujeme se s množinami, SNTL, Praha 1982

[3] K. Devlin, Jazyk matematiky, Argo, Dokořán, Praha 2002.

[4] E. Fuchs, Teorie množin pro učitele, Masarykova univerzita, Brno 1999.

[5] P. Horák, Základy matematiky, PřF MU Brno (příp. též starší vydání skript Algebra a teoretická aritmetika od téhož autora, které je svým obsahem podobné).

[6] L. Kosmák, Množinová algebra, Masarykova univerzita, Brno 1995.

[7] J. Kuben, P. Šarmanová, Diferenciální počet funkcí jedné proměnné, VŠB TU Ostrava 2006.

[8] J. Polák, Přehled středoškolské matematiky (7. vydání), Prometheus, Praha 2000.

Kapitola 4

Číselné obory

4.1 Intuitivní popis a úvodní poznámky

Naše definice číselných oborů jsou pouze intuitivní (podobně jako náš přístup k výrokům či množinám). Jejich přesnější konstrukce či definice (přičemž existuje více různých přístupů) jsou poněkud komplikovanější a s některými se setkáte v dalších semestrech.

- *Přirozená čísla:* $\mathbb{N} = \{1, 2, 3, \dots\}$. Někdy se do této množiny zahrnuje i 0. My to však dělat nebudeme. Někdy se značí $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

- *Celá čísla:* $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

- *Racionální čísla:* $\mathbb{Q} = \{x : x = a/b, a, b \in \mathbb{Z}, b \neq 0\}$. Bez újmy na obecnosti lze brát $b \in \mathbb{N}$. Použijeme-li pro zápis racionálního čísla zápis, kde se ve jmenovateli vyskytuje nejmenší možné kladné číslo, pak jsme jej vyjádřili v tzv. *základním tvaru.* Takové vyjádření je jednoznačné.

- *Reálná čísla:* $\mathbb{R}$. Neformálně lze tuto množinu vyjádřit několika způsoby. $\mathbb{R}$ se skládá ze dvou disjunktních podmnožin, totiž $\mathbb{Q}$ a $\mathbb{I}$, kde $\mathbb{I}$ je množina čísel iracionálních (nelze je vyjádřit jako podíl celých čísel; alternativně lze říci, že iracionální čísla lze zapsat jen takovým desetinným rozvojem, který je nekonečný a neperiodický). Existuje vzájemně jednoznačné přiřazení všech reálných čísel a všech bodů libovolné přímky. Též lze říci, že reálná čísla vyjadřují délky úseček (při zvolené jednotkové úsečce), čísla k nim opačná a nulu. Někdy se značí $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$, $\mathbb{R}^- = \{x \in \mathbb{R} : x < 0\}$.

- *Komplexní čísla:* $\mathbb{C} = \{x : x = a + ib, a, b \in \mathbb{R}\}$, kde i je imaginární jednotka, pro kterou platí $i^2 = -1$, a dále definujeme $(a+bi)+(c+di) = (a+c)+(b+d)i$, $(a+bi)(c+di) = (ab-bd)+(ad+bc)i$. Též lze definovat $\mathbb{C}$ jako $\mathbb{R}\times\mathbb{R}$ s příslušnými operacemi mezi uspořádanými dvojicemi. Pro $z \in \mathbb{C}$ se vyjádření $z = a + bi$ nazývá *algebraický tvar*, kde a je *reálná část*, b je *imaginární část*. Komplexní čísla lze geometricky znázornit jako body v *Gaussově rovině*: osa x je reálná osa, osa y je imaginární osa.

Platí tyto inkluze
$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

4.2 Některé vybrané vlastnosti čísel

Základní operace s čísly (sčítání, násobení, umocňování atd.) a jejich vlastnosti zde nebudeme pro jednotlivé číselné obory detailně opakovat. Předpokládá se, že studenti matematických oborů s tímto nemají problém. Bylo by fajn, kdyby se mezi čtenáři tohoto textu nevyskytovali studenti používající příšernosti typu $\frac{1}{a+b} = \frac{1}{a} + \frac{1}{b}$.

Poznamenejme pouze, že ve všech uvedených číselných oborech je možno čísla sčítat a násobit, přičemž jak sčítání, tak násobení jsou komutativní, asociativní a platí distributivní zákon. Navíc v $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ke každému číslu existuje číslo opačné, zatímco v $\mathbb{N}$ tomu tak není. Dále v $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ke každému nenulovému číslu existuje číslo převrácené, zatímco v $\mathbb{N}, \mathbb{Z}$ tomu tak není. Čísla množin $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ lze uspořádat „podle velikosti“ (tzn. zavést symboly $\leq, <$).

Zejména zde uvedeme pojmy a vlastnosti, které nemusejí být standardně uváděny na středních školách, a přitom se nám budou později velmi hodit.

Začněme s připomínkou, že pro $\mathbb{N}$ platí princip úplné indukce: Je-li $M \subseteq \mathbb{N}$ taková, že $1 \in M$ a s každým $n \in M$ obsahuje množina M i číslo $n + 1$, pak $M = \mathbb{N}$. Lze ukázat, že $\mathbb{N}$ je nejmenší množina (vzhledem k inkluzi) ze všech množin $A \subseteq \mathbb{R}$ s vlastnostmi $1 \in A$ a pro každé $n \in A$ platí $n + 1 \in A$.

Následující pojem zavádíme v oboru $\mathbb{Z}$ a v budoucnu jej využijeme v souvislosti s řešením Diofantických rovnic, v souvislosti s ekvivalencemi a rozklady a v souvislosti s konečnými grupami (a modulární aritmetikou). Nejdříve připomeňme, že jsou-li $a, b \in \mathbb{Z}$, pak říkáme, že *a dělí b* a píšeme $a|b$, jestliže $\exists z \in \mathbb{Z} : b = az$. Nechť $m \in \mathbb{N}$ je pevné a $a, b \in \mathbb{Z}$. Jestliže

$m|(b-a)$, pak řekneme, že čísla a, b jsou *kongruentní podle modulu* m a píšeme $a \equiv b(\operatorname{mod} m)$. Lze ukázat, že $a \equiv b(\operatorname{mod} m)$, právě když a, b dávají po dělení číslem m stejný zbytek, což je právě když a, b se liší o celočíselný násobek čísla m. Platí $a \equiv a(\operatorname{mod} m)$, $a \equiv b(\operatorname{mod} m) \Rightarrow b \equiv a(\operatorname{mod} m)$, $a \equiv b(\operatorname{mod} m) \wedge b \equiv c(\operatorname{mod} m) \Rightarrow a \equiv c(\operatorname{mod} m)$. Jestliže $a \equiv b(\operatorname{mod} m)$, $c \equiv d(\operatorname{mod} m)$, pak platí $a+c \equiv b+d(\operatorname{mod} m)$, $a-c \equiv b-d(\operatorname{mod} m)$, $a \cdot c \equiv b \cdot d(\operatorname{mod} m)$, $a^n \equiv b^n(\operatorname{mod} m)$ pro libovolné $n \in \mathbb{N}$. Nelze libovolně provádět „krácení“, např. $3 \cdot 6 \equiv 7 \cdot 6(\operatorname{mod} 8)$, ale přitom neplatí $3 \equiv 7(\operatorname{mod} 8)$. Platí však toto $a \cdot c \equiv b \cdot c(\operatorname{mod} m) \wedge c, m$ jsou nesoudělná $\Rightarrow a \equiv b(\operatorname{mod} m)$.

O množinách $\mathbb{R}, \mathbb{I}, \mathbb{Q}$ lze dokázat tuto zajímavou vlastnost: Mezi dvěma různými reálnými čísly leží jak nekonečně mnoho různých racionálních, tak i nekonečně mnoho různých iracionálních čísel.

Množinu $\mathbb{R}^* = \mathbb{R} \cup \{\infty, -\infty\}$ (kde $\infty, -\infty \notin \mathbb{R}$ a pro libovolné $x \in \mathbb{R}$ platí $-\infty < x < \infty$) nazýváme *rozšířenou množinou reálných čísel*. V množině $\mathbb{R}^*$ definujeme následující operace: $x + \infty = \infty + x = \infty$ pro $x > -\infty$, $x + (-\infty) = -\infty + x = -\infty$ pro $x < \infty$, $x \cdot (\pm\infty) = \pm\infty \cdot x = \pm\infty$ pro $x \in \mathbb{R} \cup \{\infty\}, x > 0$, $x \cdot (\pm\infty) = \pm\infty \cdot x = \mp\infty$ pro $x \in \mathbb{R} \cup \{-\infty\}, x < 0$, $\frac{x}{\infty} = \frac{x}{-\infty} = 0$ pro $x \in \mathbb{R}$, $|-\infty| = |\infty| = \infty$. Nedefinují se tyto operace: $\infty + (-\infty), -\infty + \infty, 0 \cdot (\pm\infty), \pm\infty \cdot 0, \frac{\pm\infty}{\pm\infty}$ a $\frac{x}{0}$ pro $x \in \mathbb{R}^*$. Intervaly definujeme takto:

$$
\begin{aligned}
&\text{Pro } a, b \in \mathbb{R}^*, a < b, \text{ je } (a, b) = \{x \in \mathbb{R} : a < x < b\},\\
&\text{pro } a, b \in \mathbb{R}, a < b, \text{ je } \langle a, b\rangle = \{x \in \mathbb{R} : a \leq x \leq b\},\\
&\text{pro } a \in \mathbb{R}, b \in \mathbb{R}^*, a < b, \text{ je } \langle a, b) = \{x \in \mathbb{R} : a \leq x < b\},\\
&\text{pro } a \in \mathbb{R}^*, b \in \mathbb{R}, a < b, \text{ je } (a, b\rangle = \{x \in \mathbb{R} : a < x \leq b\}.
\end{aligned}
$$

Zřejmě $(-\infty, \infty) = \mathbb{R}$. Někde v literatuře se též definuje např. pro $a < \infty$ $(a, \infty\rangle = \{x \in \mathbb{R}^* : a < x \leq \infty\}$ atd.

Následující pojmy budou později diskutovány v souvislosti s tzv. uspořádanými množinami. My si zde nyní uvedeme specifikace pro případ množiny $\mathbb{R}$ ($\mathbb{R}^*$). Nechť $M \subseteq \mathbb{R}^*$, $a, b \in \mathbb{R}^*$. Řekneme, že b je *horní závora množiny* M, jestliže $\forall x \in M : x \leq b$. Řekneme, že a je *dolní závora množiny* M, jestliže $\forall x \in M : x \geq a$. Řekneme, že b je *maximum množiny* M, jestliže b je horní závora množiny M a $b \in M$ (píšeme $b = \max M$). Řekneme, že a je *minimum množiny* M, jestliže a je dolní závora množiny M a $a \in M$ (píšeme $a = \min M$). Označme $U(M)$ množinu všech horních závor a $L(M)$ množinu všech dolních závor. Řekneme, že b je *supremum množiny* M (píšeme $b = \sup M$), jestliže $b = \min U(M)$. Řekneme, že a je *infimum* *množiny* M (píšeme $a = \inf M$), jestliže $a = \max L(M)$. Pro $M \neq \emptyset$ platí $\inf M \leq \sup M$. Dále platí $\inf \emptyset = \max \mathbb{R}^* = \infty > -\infty = \min \mathbb{R}^* = \sup \emptyset$. Platí, že každá množina $M \subseteq \mathbb{R}^*$ má v $\mathbb{R}^*$ supremum a infimum. Dále platí, že každá neprázdná shora ohraničená množina $M \subseteq \mathbb{R}$ má v $\mathbb{R}$ supremum (ekvivalentně, každá neprázdná zdola ohraničená množina $M \subseteq \mathbb{R}$ má v $\mathbb{R}$ infimum). Tato posledně jmenovaná vlastnost množiny $\mathbb{R}$ (při axiomatickém zavádění $\mathbb{R}$ je to vlastně jeden z axiomů, tzv. úplnost) je velmi významná. Populárně řečeno, říká, že v $\mathbb{R}$ nejsou žádné „díry“ ani „mezery“. Např. pro množinu $\mathbb{Q}$ tato vlastnost neplatí. Uvědomte si jaké platí vztahy mezi infimem a minimem, resp. mezi supremem a maximem.

Nyní si připomeňme pojem *absolutní hodnoty* čísla $a \in \mathbb{R}$:

$$|a| = \begin{cases} a & \text{jestliže } a \geq 0 \\ -a & \text{jestliže } a < 0. \end{cases}$$

Platí tzv. *trojúhelníková nerovnost* $|a + b| \leq |a| + |b|$. Číslo $|a - b|$ (resp. $|b-a|$) je rovno vzdálenosti bodů a a b na číselné ose. Zejména v matematické analýze se nám budou velmi hodit následující souvislosti mezi nerovnostmi s absolutními hodnotami, nerovnostmi bez absolutních hodnot a intervaly (pro daná $a, b \in \mathbb{R}, b > 0$), např. $\{x \in \mathbb{R} : |x - a| < b\} = \{x \in \mathbb{R} : a - b < x < a + b\} = (a - b, a + b)$, či $\{x \in \mathbb{R} : |x - a| > b\} = \{x \in \mathbb{R} : x < a - b \vee x > a + b\} = (-\infty, a - b) \cup (a + b, \infty)$. Podobně pro neostré nerovnosti.

Nakonec uvažujme množinu $\mathbb{C}$. Číslo $a - bi$ se nazývá *komplexně sdružené* k číslu $z = a + bi$ (označ. $\bar{z}$). *Absolutní hodnota* čísla $z = a + bi$ je definovaná vztahem $|z| = \sqrt{a^2 + b^2} = \sqrt{z \cdot \bar{z}}$. Pro *goniometrický tvar* čísla $z = a + bi$ platí $z = |z|(\cos \varphi + i \sin \varphi)$, kde tzv. *argument* φ (označ. $\varphi = \arg z$) je úhel určený (až na celočíselný násobek 2π) vztahy $\cos \varphi = a/|z|$, $\sin \varphi = b/|z|$. *Hlavní hodnota argumentu* čísla z je $\varphi \in (-\pi, \pi\rangle$ (určena jednoznačně). Nechť $n \in \mathbb{N}$. Pak n-tou mocninu čísla $z \in \mathbb{C}$ lze počítat podle *Moivreovy věty* $z^n = |z|^n(\cos n\varphi + i \sin n\varphi)$. Pro $n \in \mathbb{N}$ a $z \in \mathbb{C}$ existuje právě n různých hodnot komplexní n-té odmocniny čísla z; ta jsou dána vzorcem $\sqrt[n]{|z|}[\cos(\varphi/n + 2k\pi/n) + i \sin(\varphi/n + 2k\pi/n)]$, $k = 0, 1, \ldots, n-1$. Zakončeme tuto kapitolu zmínkou o elegantním *Eulerově vzorci* $e^{ix} = \cos x + i \sin x$, který platí pro každé $x \in \mathbb{R}$. Speciálně pro $x = \pi$ dostaneme $e^{i\pi} + 1 = 0$. Tato zajímavá rovnost dává do souvislosti tři základní aritmetické operace (součet, součin, mocnina) s pěti základními (nejznámějšími) matematickými konstantami $(e, \pi, i, 0, 1)$. Přitom se v této rovnosti vyskytuje každá z operací i každá z konstant právě jednou a žádné jiné operace ani jiné konstanty se v ní nevyskytují.

4.3 Literatura

[1] I. Bušek, E. Calda, Matematika pro gymnázia. Základní poznatky z matematiky (3. vydání), Prometheus, Praha 2006.

[2] K. Devlin, Jazyk matematiky, Argo, Dokořán, Praha 2002.

[3] P. Horák, Základy matematiky, PřF MU Brno (příp. též starší vydání skript Algebra a teoretická aritmetika od téhož autora, které je svým obsahem podobné).

[4] R. Kučera, L. Skula, Číselné obory, PřF MU Brno 1998.

[5] J. Kuben, P. Šarmanová, Diferenciální počet funkcí jedné proměnné, VŠB TU Ostrava 2006.

[6] J. Polák, Přehled středoškolské matematiky (7. vydání), Prometheus, Praha 2000.

Kapitola 5

Relace

5.1 Relace mezi množinami

Začneme definicí. Nechť A, B jsou množiny. Pak libovolnou množinu

$$\varrho \subseteq A \times B$$

nazýváme *relací mezi množinami* A a B (záleží na pořadí). Jestliže $(a, b) \in \varrho$ (resp. $(a, b) \notin \varrho$), pak říkáme, že prvek a je v relaci ϱ (resp. není v relaci ϱ) s prvkem b. Vztah $(a, b) \in \varrho$ někdy stručně zapisujeme jako $a\varrho b$. Místo $(a, b) \notin \varrho$ pak někdy píšeme $a\bar{\varrho}b$.

Poznámka 5.1. Někdy se při definování postupuje poněkud formálněji: Je-li $M \subseteq A \times B$, pak uspořádanou dvojici $\varrho = ((A, B), M)$ nazýváme relací. Množina M se nazývá grafem.

Relace $\varrho = \emptyset$ je tzv. *prázdná relace mezi* A, B, relace $\varrho = A \times B$ je tzv. *univerzální relace mezi* A, B.

Poznámka 5.2. Pojem relace mezi A, B úzce souvisí s těmito množinami. Nechť ϱ je relace mezi A, B a σ je relace mezi C, D. Pak *relace* ϱ *a* σ *se sobě rovnají* (píšeme $\varrho = \sigma$), jestliže $\varrho = \sigma, A = C, B = D$. Při formálnější definici by rovnosti $A = C, B = D$ byly jejím přímým důsledkem.

Nechť ϱ je relace mezi A, B. Potom se množina $\operatorname{Dom} \varrho = \{x \in A : \exists y \in B$ tak, že $x\varrho y\}$ nazývá *definiční obor relace* ϱ. Množina $\operatorname{Ran} \varrho = \{y \in B : \exists x \in A$ tak, že $x\varrho y\}$ se nazývá *obor hodnot relace* ϱ, případně *obraz relace* ϱ.

Pozor: v literatuře se lze setkat s odlišným označováním definičního oboru a oboru hodnot.

Pro větší názornost si můžeme relace mezi množinami znázorňovat graficky: body v rovině (znázorňující prvky množin A, B) spojíme orientovanou šipkou, právě když jsou v relaci.

Relace lze skládat v následujícím smyslu. Nechť ϱ je relace mezi A, B a σ je relace mezi C, D. Pak relace

$$\sigma \circ \varrho = \{(x, y) \in A \times C : \exists b \in B \text{ tak, že } x\varrho b \wedge b\sigma y\}$$

(čti: „σ po ϱ“) se nazývá *složená relace* z relací ϱ a σ (v tomto pořadí).

Komutativita (tj. $\varrho \circ \sigma = \sigma \circ \varrho$) neplatí. Najděte si vhodný příklad (uvědomte si přitom, jaký vztah musí splňovat A, B, C). Asociativita (tj. $\tau \circ (\sigma \circ \varrho) = (\tau \circ \sigma) \circ \varrho$ pro relaci ϱ mezi A, B, relaci σ mezi B, C a relaci τ mezi C, D) platí. Dokažte si ji (rovnost dokazujeme jako množinovou rovnost).

Dále definujeme tzv. inverzní relaci. Nechť ϱ je relace mezi A, B. Potom relace ϱ^{-1} mezi B, A definovaná vztahem

$$\varrho^{-1} = \{(b, a) \in B \times A : a\varrho b\}$$

se nazývá *inverzní relace k relaci* ϱ. Jak vypadají grafická znázornění relací ϱ, ϱ^{-1}?

Zřejmě platí $(\varrho^{-1})^{-1} = \varrho$. Dále si dokažte (jako množinovou rovnost), že $(\sigma \circ \varrho)^{-1} = \varrho^{-1} \circ \sigma^{-1}$.

5.2 Relace na množině

Nechť A je množina. Pak libovolnou množinu

$$\varrho \subseteq A^2$$

nazýváme *relací na množině* A. Množinu A s relací ϱ značíme (A, ϱ). Poněvadž jde o speciální případ relace mezi A, B, kde $A = B$, platí všechny výsledky předchozí podkapitoly i pro relace na množině.

Poznámka 5.3. Relace $\varrho \subseteq A^2$ se též někdy nazývá *binární relace na* A. Podobně lze definovat *n-ární relaci na A* jako libovolnou podmnožinu množiny A^n (pro $n = 1$ tzv. unární relaci, pro $n = 2$ binární relaci, pro $n = 3$ tzv. ternární relaci). Protože však zde pracujeme převážně s binárními relacemi, mluvíme stručně o relacích.

Pro libovolnou množinu A je relace $\mathrm{id}_A = \{(x,x) : x \in A\}$ nazývána *identickou* nebo *diagonální* relací na A.

Relaci na množině (zejména, je-li konečná) lze znázornit graficky (pomocí (nejen) uzlového grafu) či tabulkou. Později uvidíme, že některé speciální typy relací je výhodné znázorňovat i jiným způsobem.

Definujeme tyto základní vlastnosti relací na množině. Nechť (A, ϱ) je množina s relací. Řekneme, že relace ϱ je

- *reflexivní*, jestliže: $x \in A \Rightarrow x\varrho x$
- *symetrická*, jestliže: $x, y \in A \wedge x\varrho y \Rightarrow y\varrho x$
- *antisymetrická*, jestliže: $x, y \in A \wedge x\varrho y \wedge y\varrho x \Rightarrow x = y$
- *tranzitivní*, jestliže: $x, y, z \in A \wedge x\varrho y \wedge y\varrho z \Rightarrow x\varrho z$
- *úplná*, jestliže: $x, y \in A \Rightarrow x\varrho y \vee y\varrho x$

Promyslete si, jak se tyto vlastnosti (kromě tranzitivity, kde je situace složitější) poznají z uzlového grafu a z tabulky relace; např při reflexivitě je v grafu každý bod opatřen smyčkou a v hlavní diagonále tabulky jsou samé jedničky atd.

Výše definované vlastnosti lze charakterizovat i jiným způsobem (někdy v literatuře jsou některé z následujících vztahů – díky ekvivalenci – užívány jako definice). Pokuste se následující ekvivalence dokázat. Nechť (A, ϱ) je množina s relací. Potom platí:

- ϱ je reflexivní $\Leftrightarrow \mathrm{id}_A \subseteq \varrho$
- ϱ je symetrická $\Leftrightarrow \varrho \subseteq \varrho^{-1}$
- ϱ je antisymetrická $\Leftrightarrow \varrho \cap \varrho^{-1} \subseteq \mathrm{id}_A$
- ϱ je tranzitivní $\Leftrightarrow \varrho \circ \varrho \subseteq \varrho$
- ϱ je úplná $\Leftrightarrow \varrho \cup \varrho^{-1} = A \times A$

Závěrem poznamenejme, že symetrie a antisymetrie se navzájem nevylučují (např. id_A). Úplná relace musí být vždy reflexivní.

5.3 Literatura

[1] B. Balcar, P. Štěpánek, Teorie množin, Academia, Praha 1986.

[2] J. Bečvář a kol., Seznamujeme se s množinami, SNTL, Praha 1982

[3] P. Horák, Základy matematiky, PřF MU Brno (příp. též starší vydání skript Algebra a teoretická aritmetika od téhož autora, které je svým obsahem podobné).

[4] L. Kosmák, Množinová algebra, Masarykova univerzita, Brno 1995.

Kapitola 6

Zobrazení

6.1 Základní pojmy

Nechť A, B jsou množiny a f je relace mezi A, B splňující vlastnost:

$$\text{pro každé } x \in A \text{ existuje právě jedno } y \in B \text{ tak, že } (x, y) \in f. \tag{6.1}$$

Pak se tato relace nazývá *zobrazení množiny A do množiny B*. Tuto relaci obvykle zapisujeme symbolem $f : A \to B$. Poznamenejme, že $\operatorname{Dom} f = A$. Místo $(x, y) \in f$ píšeme $f(x) = y$, přičemž y se nazývá *obraz prvku x* (při zobrazení f) a x se nazývá *vzor prvku y* (při zobrazení f).

Poznámka 6.1. (i) Někdy se zobrazení definuje intuitivně jako *předpis*, který každému prvku množiny A přiřazuje právě jeden prvek množiny B. Tato definice však nemůže být zcela přesná, neboť používá mlhavého (nedefinovaného) pojmu „předpis“. Nové pojmy lze definovat pouze na základě již dříve definovaných pojmů. Náš přístup k definici pomocí relace tento problém odstraňuje.

(ii) Někdy se používá (obecnějšího) pojmu, totiž *zobrazení z množiny A do množiny B*, kde (6.1) je nahrazena (obecnější) vlastností: pro každé $x \in A$ existuje nejvýše jedno $y \in B$ tak, že $(x, y) \in f$.

K zadání zobrazení je potřeba zadat množinu A (definiční obor), množinu B a předpis (tj. vhodnou relaci) f. Přitom předpis lze zadat různými způsoby.

V některých speciálních případech užíváme pro pojem zobrazení jiného výrazu: např. $f : A \to \mathbb{R}$, kde $A \subseteq \mathbb{R}$ se nazývá *reálná funkce (jedné) reálné* *proměnné* nebo $f : \mathbb{N} \to B$ se nazývá *posloupnost* (místo $f(n)$ píšeme f_n) apod.

Zobrazení $f : A \to B,\ g : C \to D$ *jsou si rovna*, právě když $A = C \wedge B = D \ \wedge\ f(x) = g(x)$ pro každé $x \in A$.

Naše definice zobrazení připouští $A = \emptyset$ nebo $B = \emptyset$. Je-li $A = \emptyset$ a B libovolná, pak existuje právě jedno zobrazení $\emptyset \to B$, které se nazývá *prázdné zobrazení*. Je-li $A \neq \emptyset$ a $B = \emptyset$, potom neexistuje zobrazení $A \to \emptyset$.

Pro *množinu všech zobrazení* $A \to B$ užíváme označení $B^A = \{f|f : A \to B\}$. Platí $|A| = n, |B| = m \Rightarrow |B^A| = m^n$ (což jistým způsobem odůvodňuje zavedené označení).

6.2 Injekce, surjekce, bijekce

Pro zobrazení definujeme následující důležité vlastnosti. Nechť $f : A \to B$ je zobrazení. Zobrazení f se nazývá

- *injektivní* (nebo též *prosté*), jestliže každý prvek z množiny B má nejvýše jeden vzor (při zobrazení f).
- *surjektivní* (nebo též *na*), jestliže každý prvek z množiny B má alespoň jeden vzor (při zobrazení f).
- *bijektivní* (nebo též *vzájemně jednoznačné*), jestliže je zároveň injektivní a surjektivní.

Často říkáme těmto zobrazením stručně injekce, surjekce, bijekce.

Rozmyslete si, jak postupujeme při důkazu injektivity, resp. surjektivity zobrazení.

Jsou-li A, B konečné množiny, kde $|A| = n, |B| = m$, potom platí následující ekvivalence: $\exists$ injekce $f : A \to B \Leftrightarrow n \leq m$; $\exists$ surjekce $f : A \to B \Leftrightarrow n \geq m$; $\exists$ bijekce $f : A \to B \Leftrightarrow n = m$. Později využijeme zobrazení (mimo jiné) k zavedení a studiu pojmu „mohutnost množiny“ (kde množina může být i nekonečná) a navíc budeme schopni se oprostit od představy, kterou si nevědomky přinášíme již ze základní školy, a sice, že počet prvků množiny je číslo. Zároveň uvidíme, že není možné přenášet všechny vžité (a správné!) představy o konečných množinách na množiny nekonečné.

Nakonec poznamenejme, že pokud $|A| = |B| = m$, potom existuje právě $m!$ navzájem různých bijektivních zobrazení.

6.3 Inverzní a složené zobrazení

Nyní budeme specifikovat pojmy, které známe už z kapitoly o relacích, totiž inverzi a skládání.

Nechť $f : A \to B$ je bijekce (uvědomte si, že inverzní relace k zobrazení není obecně zobrazení). Potom definujeme zobrazení $f^{-1} : B \to A$ takto: pro každé $y \in B$ klademe $f^{-1}(y) = x$, kde $x \in A$ je vzorem prvku y při zobrazení f (tj. $f(x) = y$). Zobrazení f^{-1} se nazývá *inverzní zobrazení* k f.

Zřejmě f^{-1} je bijekce a $(f^{-1})^{-1} = f$.

Nechť $f : A \to B$ a $g : B \to C$ jsou zobrazení. Potom zobrazení $g \circ f : A \to C$ [čti: „g po f“] definované předpisem $(g \circ f)(x) = g(f(x))$ pro každé $x \in A$ se nazývá *složené zobrazení* (ze zobrazení f a g, v tomto pořadí).

Místo $g \in B \to C$ lze (obecněji) uvažovat $g : D \to C$. Aby však v tomto případě bylo skládání možné, je potřeba předpokládat $\operatorname{Ran} f \subseteq D (= \operatorname{Dom} g)$.

Pro skládání zobrazení neplatí komutativní zákon a platí asociativní zákon.

Pro $f : A \to B$ platí $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$. Je-li navíc f bijekce, potom $f^{-1} \circ f = \mathrm{id}_A$ a $f \circ f^{-1} = \mathrm{id}_B$.

Pro skládání zobrazení a vlastnosti injektivity a surjektivity platí následující vztahy (pokuste se je dokázat). Nechť $f : A \to B,\ g : B \to C$ jsou zobrazení. Potom:

$$f, g \text{ jsou injekce } \Rightarrow g \circ f \text{ je injekce}$$
$$f, g \text{ jsou surjekce } \Rightarrow g \circ f \text{ je surjekce}$$
$$g \circ f \text{ je injekce } \Rightarrow f \text{ je injekce}$$
$$g \circ f \text{ je surjekce } \Rightarrow g \text{ je surjekce}$$

Dále lze ukázat (pokuste se o důkaz s využitím výše uvedených výsledků) následující ekvivalenci. Nechť $f : A \to B,\ g : B \to A$. Potom $g \circ f = \mathrm{id}_A \ \wedge\ f \circ g = \mathrm{id}_B \Leftrightarrow f, g$ jsou bijekce $\wedge\ g = f^{-1}$.

6.4 Literatura

[1] B. Balcar, P. Štěpánek, Teorie množin, Academia, Praha 1986.

[2] J. Bečvář a kol., Seznamujeme se s množinami, SNTL, Praha 1982

[3] P. Horák, Základy matematiky, PřF MU Brno (příp. též starší vydání skript Algebra a teoretická aritmetika od téhož autora, které je svým obsahem podobné).

[4] L. Kosmák, Množinová algebra, Masarykova univerzita, Brno 1995.

Kapitola 7

Uspořádání

7.1 Základní pojmy

Nechť (A, ϱ) je množina s relací. Jestliže ϱ je reflexivní, antisymetrická a tranzitivní, pak se tato relace nazývá *uspořádání* (na množině A) a (A, ϱ) se nazývá *uspořádaná množina*. Je-li navíc ϱ úplná, pak se nazývá *lineární uspořádání* (na množině A) a (A, ϱ) se nazývá *lineárně uspořádaná množina* nebo *řetězec*.

Terminologie v teorii uspořádání není jednotná. Někdy se např. užívá název *částečné uspořádání* místo uspořádání a *uspořádáním* se rozumí lineární uspořádání. Někdy se místo lineární uspořádání resp. lineárně uspořádaná množina říká *úplné uspořádání* resp. *úplně uspořádaná množina*.

Relaci uspořádání obvykle značíme symbolem $\leq$ („menší nebo rovno"), případně symbolem $\preceq$. Obecně tento symbol nemá nic společného se srovnáváním čísel podle velikosti (v podstatě je tím však motivován). Místo $x \leq y$ lze psát (podle potřeby) $y \geq x$. Místo $x \leq y \wedge x \neq y$ stručně píšeme $x < y$ (nebo $y > x$).

Uspořádanou množinu $(A, \leq)$ lze často znázorňovat graficky pomocí tzv. *hasseovského diagramu*: prvky množiny A znázorníme jako body v rovině, přičemž je-li $x < y$, pak bod x nakreslíme níže než bod y. Dále dva body x, y spojíme úsečkou právě tehdy, když $x < y$ a $\nexists z \in A : x < z \wedge z < y$ (tj. neexistuje bod mezi x a y). V podstatě jde o zjednodušený uzlový graf, kde jsou vynechány „zbytečné" šipky a orientace šipek. Uvedená konstrukce nedefinuje jednoznačně „tvar" diagramu. Známe-li hasseovský diagram, lze z něj pak relaci $\leq$ jednoznačně zpětně zrekonstruovat.

7.2 Význačné prvky v uspořádaných množinách

Nechť $(A, \leq)$ je uspořádaná množina. Prvek $a \in A$ se nazývá

- *nejmenší*, jestliže pro každé $x \in A$ je $a \leq x$.
- *největší*, jestliže pro každé $x \in A$ je $x \leq a$.
- *minimální*, jestliže neexistuje $x \in A$ takové, že $x < a$.
- *maximální*, jestliže neexistuje $x \in A$ takové, že $a < x$.

Prvky $x, y \in A$ se nazývají *srovnatelné*, jestliže $x \leq y$ nebo $y \leq x$. V opačném případě se prvky x, y nazývají *nesrovnatelné*.

Výše definované prvky mají následující „očekávatelné" vlastnosti (pokuste se je dokázat): Nechť $(A, \leq)$ je uspořádaná množina. Potom

- $(A, \leq)$ má nejvýše jeden největší a nejvýše jeden nejmenší prvek.
- $a \in A$ je nejmenší [největší] prvek $\Rightarrow$ a je minimální [maximální] prvek a žádné další minimální [maximální] prvky v $(A, \leq)$ neexistují.
- Množina $(A, \leq)$ je lineárně uspořádaná $\Leftrightarrow$ každé dva prvky $x, y \in A$ jsou srovnatelné.
- Nechť $(A, \leq)$ je řetězec. Potom $a \in A$ je minimální [maximální] $\Leftrightarrow$ a je nejmenší [největší].

Podobně jako jsme to dříve dělali v případě (uspořádané) množiny $\mathbb{R}$ resp. $\mathbb{R}^*$, lze i v obecné uspořádané množině zavést pojmy jako horní a dolní závora, supremum a infimum a studovat jejich vlastnosti. S touto látkou se však podrobněji setkáte později.

7.3 Literatura

[1] B. Balcar, P. Štěpánek, Teorie množin, Academia, Praha 1986.

[2] J. Bečvář a kol., Seznamujeme se s množinami, SNTL, Praha 1982

[3] P. Horák, Základy matematiky, PřF MU Brno (příp. též starší vydání skript Algebra a teoretická aritmetika od téhož autora, které je svým obsahem podobné).

[4] L. Kosmák, Množinová algebra, Masarykova univerzita, Brno 1995.

Kapitola 8

Relace ekvivalence a rozklady

8.1 Relace ekvivalence

Jestliže (A, ϱ) je množina s relací, která je reflexivní, symetrická a tranzitivní, pak se tato relace nazývá *ekvivalence* (na množině A).

Relaci ekvivalence obvykle značíme symbolem $\sim$.

Pozor na terminologii: ekvivalencí též nazýváme logickou spojku $\Leftrightarrow$. Z kontextu však vždy bude jasné, kterou ekvivalenci máme na mysli.

Příklad 8.1. (i) Nechť $A \neq \emptyset$ je libovolná množina. Potom id_A a $A \times A$ jsou relacemi ekvivalence na A. Označíme-li $\mathcal{E}(A)$ množinu všech relací ekvivalence na A, potom $(\mathcal{E}(A), \subseteq)$ je uspořádaná množina s nejmenším prvkem id_A a největším prvkem $A \times A$.

(ii) Relace kongruence podle modulu m je relací ekvivalence na $\mathbb{Z}$.

Platí: ϱ je ekvivalence na $A \Rightarrow \varrho^{-1}$ je ekvivalence na A. Dokažte si. Dále lze například ukázat, že průnik libovolného systémů ekvivalencí je ekvivalence.

8.2 Rozklady

Nechť $A \neq \emptyset$ je libovolná množina. Pak systém $\mathcal{M}$ neprázdných podmnožin množiny A se nazývá *rozklad na množině* A, jestliže splňuje tyto podmínky: (i) $X, Y \in \mathcal{M} \wedge X \neq Y \Rightarrow X \cap Y = \emptyset$, (ii) $\bigcup\limits_{X \in \mathcal{M}} X = A$ [připomeňme, že $\bigcup\limits_{X \in \mathcal{M}} X$ je sjednocení všech množin ze systému $\mathcal{M}$]. Prvky systému $\mathcal{M}$ se nazývají *třídy rozkladu* $\mathcal{M}$.

Dokazujeme-li, že $\mathcal{M}$ je rozklad na A, pak obvykle ověřujeme následující tři podmínky (promyslete si, proč): (i) $X \in \mathcal{M} \Rightarrow \emptyset \neq X \subseteq A$, (ii) $X, Y \in \mathcal{M}$ a $X \cap Y \neq \emptyset \Rightarrow X = Y$, (iii) $A \subseteq \bigcup\limits_{X \in \mathcal{M}} X$.

Příklad 8.2. (i) Dva nejjednodušší typy rozkladů na $A \neq \emptyset$ jsou $\mathcal{M} = \{\{x\} : x \in A\}$ a $\mathcal{M} = \{A\}$.

(ii) Nechť $n \in \mathbb{N}$ je pevné. Označme $C_i = \{x \in \mathbb{Z} : x \equiv i(\bmod m)\}$, $i = 0, 1, \ldots, m-1$. Pak množina C_i se nazývá *zbytková třída podle modulu* m. Označme $\mathbb{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$. Potom $\mathbb{Z}_m$ je rozklad na $\mathbb{Z}$. Promyslete si, proč nemůže platit např. vztah $\mathbb{Z}_3 \subseteq \mathbb{Z}_4$ (i když k platnosti takového vztahu „svádí“ definice pomocí zbytkových tříd).

8.3 Vztahy mezi ekvivalencemi a rozklady

Z výše uvedených příkladů lze intuitivně vytušit platnost následujících obecných tvrzení, jejichž přesné důkazy lze nalézt v literatuře.

Platí: Nechť $\sim$ je relace ekvivalence na A. Pro $a \in A$ položme $X_a = \{x \in A : x \sim a\}$. Potom systém množin $\{X : \exists a \in A$ tak, že $X = X_a\}$ je rozklad na množině A. Tento systém označujeme symbolem $A/\!\sim$ a říkáme, že $A/\!\sim$ je *rozklad příslušný ekvivalenci* $\sim$.

Příklad 8.3. (i) Nechť $A \neq \emptyset$ je libovolná množina. a) Jestliže $\sim = \mathrm{id}_A$, potom $A/\!\sim = \{\{x\} : x \in A\}$. b) Jestliže $\sim = A \times A$, potom $A/\!\sim = \{A\}$

(ii) Nechť $A = \mathbb{Z}$. Jestliže $\sim = \equiv$ (kde $\equiv$ je relace kongruence podle modulu m), potom $\mathbb{Z}/\!\equiv\, = \mathbb{Z}_m$.

Platí: Nechť $\mathcal{M}$ je rozklad na A. Pro $a, b \in A$ položíme $a \sim_{\mathcal{M}} b \Leftrightarrow \exists$ třída $X \in \mathcal{M}$ tak, že $a, b \in X$. Pak relace $\sim_{\mathcal{M}}$ je relací ekvivalence na A. Tuto relaci nazýváme *ekvivalence příslušná rozkladu* $\mathcal{M}$.

Příklad 8.4. Nechť $A \neq \emptyset$ je libovolná množina. a) Jestliže $\mathcal{M} = \{\{x\} : x \in A\}$, potom $\sim_{\mathcal{M}} = \mathrm{id}_A$. b) Jestliže $\mathcal{M} = \{A\}$, potom $\sim_{\mathcal{M}} = A \times A$.

Není obtížné vysledovat následující fakt: Vyjdeme-li od jisté ekvivalence na A, utvoříme-li rozklad na A, přísušný této ekvivalenci a potom utvoříme ekvivalenci na A, příslušnou tomuto rozkladu, skončíme u původní ekvivalence, od níž jsme vyšli. Podobně, začneme-li rozkladem, dojdeme přes příslušnou ekvivalenci opět k původnímu rozkladu. Můžeme tedy říci, že se tímto způsobem ekvivalence a rozklady vzájemně určují. Přesně platí tyto vztahy: Nechť $A \neq \emptyset$ je libovolná neprázdná množina. Potom

- $\sim$ je ekvivalence na $A \Rightarrow \sim_{A/\sim} = \sim$.
- $\mathcal{M}$ je rozklad na $A \Rightarrow A/\sim_{\mathcal{M}} = \mathcal{M}$.

Uvědomte si, že tato dvě tvrzení jsou vlastně množinové rovnosti a také se tak dokazují.

Promyslete si příklady různých situací z běžného života, kde se setkáváme s ekvivalencemi a rozklady (aniž si to uvědomujeme).

8.4 Literatura

[1] B. Balcar, P. Štěpánek, Teorie množin, Academia, Praha 1986.

[2] J. Bečvář a kol., Seznamujeme se s množinami, SNTL, Praha 1982

[3] P. Horák, Základy matematiky, PřF MU Brno (příp. též starší vydání skript Algebra a teoretická aritmetika od téhož autora, které je svým obsahem podobné).

[4] L. Kosmák, Množinová algebra, Masarykova univerzita, Brno 1995.

Kapitola 9

Reálné funkce reálné proměnné

9.1 Základní pojmy

Nechť $f : A \to B$ je zobrazení. Jestliže $\emptyset \neq A \subseteq \mathbb{R}$ a $B = \mathbb{R}$, pak toto zobrazení nazýváme *reálnou funkcí jedné reálné proměnné* (dále jen *funkcí*).

Množina A se nazývá *definiční obor* funkce f a značí se $D(f)$. Množina $\{y \in \mathbb{R} : \exists x \in D(f)$ tak, že $y = f(x)\}$ se nazývá *obor hodnot* funkce f a značí se $H(f)$. (Jedná se zřejmě o speciální případy výše definovaných množin $\operatorname{Dom} f$ resp. $\operatorname{Ran} f$.)

K zadání funkce je nutné uvést $D(f)$ a pravidlo (předpis), které každému $x \in D(f)$ přiřadí právě jedno $y \in H(f)$.

Často se ovšem stává, že $D(f)$ není výslovně uveden. Pak za definiční obor pokládáme množinu všech $x \in \mathbb{R}$ takových, pro která má daný předpis „smysl“.

Rovností funkcí f a g máme na mysli toto: $f = g \Leftrightarrow ((D(f) = D(g)) \wedge (\forall x \in D(f) : f(x) = g(x)))$.

Grafem funkce $f : D(f) \to \mathbb{R}$ rozumíme množinu bodů $\{(x, f(x)) \in \mathbb{R}^2 : x \in D(f)\}$.

9.2 Základní vlastnosti funkcí

Funkce f se nazývá *ohraničená* (resp. *shora ohraničená*, resp. *zdola ohraničená*), je-li $H(f)$ ohraničená (resp. shora ohraničená, resp. zdola ohraničená) podmnožina množiny $\mathbb{R}$. Místo pojmu „ohraničená“ se někdy užívá pojem „omezená“.

Řekneme, že funkce f je na množině $I \subseteq D(f)$

- *rostoucí* (resp. *klesající*), jestliže $x_1, x_2 \in I$, $x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$ (resp. $f(x_1) > f(x_2)$).
- *neklesající* (resp. *nerostoucí*), jestliže $x_1, x_2 \in I$, $x_1 < x_2 \Rightarrow f(x_1) \leq f(x_2)$ (resp. $f(x_1) \geq f(x_2)$).

Funkce f se nazývá *monotonní* na I, jestliže je zde nerostoucí nebo neklesající. Funkce f se nazývá *ryze monotonní* na I, jestliže je zde rostoucí nebo klesající. Evidentně je každá ryze monotonní funkce také monotonní, ne však naopak.

Funkce f se nazývá *sudá* (resp. *lichá*), jestliže platí (i) $x \in D(f) \Rightarrow -x \in D(f)$, (ii) $f(-x) = f(x)$ (resp. $f(-x) = -f(x)$) pro každé $x \in D(f)$.

Přímo z definice plyne, že graf sudé funkce je symetrický podle osy y, graf liché funkce je symetrický podle počátku.

Nechť $p \in (0, \infty)$. Řekneme, že funkce f je *periodická* s *periodou* p (neboli p-*periodická*), jestliže platí (i) $x \in D(f) \Rightarrow x \pm p \in D(f)$, (ii) $f(x+p) = f(x)$ pro každé $x \in D(f)$.

Je lehké vidět, že je-li p perioda funkce f, je np, $n \in \mathbb{N}$, též perioda funkce f. Tedy množina P všech period periodické funkce je vždy nekonečná. Pokud existuje $\min P$, nazývá se *nejmenší perioda* funkce f (nebo také *základní perioda* či *ryzí perioda*).

9.3 Operace s funkcemi, transformace grafu

Nechť f, g jsou funkce. Potom definujeme

- *součet* $f + g$ takto: $(f+g)(x) = f(x) + g(x)$, $D(f+g) = D(f) \cap D(g)$.
- *rozdíl* $f - g$ takto: $(f-g)(x) = f(x) - g(x)$, $D(f-g) = D(f) \cap D(g)$.
- *součin* fg takto: $(fg)(x) = f(x) + g(x)$, $D(fg) = D(f) \cap D(g)$.
- *podíl* f/g takto: $(f/g)(x) = f(x)/g(x)$, $D(f/g) = D(f) \cap \{x \in D(g) : g(x) \neq 0\}$.
- *mocnina* f^g takto: $(f^g)(x) = f(x)^{g(x)}$, $D(f^g) = D(g) \cap \{x \in D(f) : f(x) > 0\}$.

Je třeba si uvědomit, že např. ve vztahu $(f+g)(x) = f(x) + g(x)$ vystupuje stejný symbol „+" v různých významech. Na levé straně rovnosti znamená operaci mezi funkcemi (tj. funkcím f, g je přiřazena funkce $f+g$) a na pravé straně má „+" význam součtu dvou reálných čísel $f(x) + g(x)$. Podobně to platí i pro ostatní operace.

Následující pojmy složené funkce a inverzní funkce jsou speciálními případy výše uvedených pojmů složeného zobrazení a inverzního zobrazení.

Předpokládejme, že f, g jsou funkce a $H(f) \subseteq D(g)$. Potom definujeme *složenou funkci* $g \circ f$ (čti: „g po f") takto: $(g \circ f)(x) = g(f(x))$, $x \in D(f)$. Funkci f nazýváme *vnitřní složka*, funkci g nazýváme *vnější složka* složené funkce $g \circ f$. Zřejmě $D(g \circ f) = D(f)$.

Poznámka 9.1. V podstatě není nezbytně nutné předpokládat $H(f) \subseteq D(g)$. Potom je však potřeba uvažovat předpis $(g \circ f)(x) = g(f(x))$ pro x taková, že $x \in D(f) \wedge f(x) \in D(g)$ (k tomu samozřejmě potřebujeme $H(f) \cap D(g) \neq \emptyset$). V tomto případě je $D(g \circ f)$ obecně pouze částí $D(f)$.

Operaci skládání lze postupně aplikovat na více funkcí, např. $(h \circ g \circ f)(x) = h(g(f(x)))$.

Dokažte si, že jestliže f, g jsou funkce obě prosté, resp. obě rostoucí, resp. obě sudé, resp. obě liché, pak funkce $g \circ f$ má také tuto vlastnost. Je-li f klesající a g rostoucí, potom $g \circ f$ i $f \circ g$ jsou klesající. Je-li f sudá a g lichá, potom $g \circ f$ i $f \circ g$ jsou sudé.

Připomeňme, že f je prostá (injektivní), jestliže platí $x_1, x_2 \in D(f)$, $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Nechť f je prostá funkce. Funkce f^{-1} se nazývá *funkce inverzní k funkci* f, jestliže $D(f^{-1}) = H(f)$, (ii) pro každé $y \in D(f^{-1})$ platí $f^{-1}(y) = x \Leftrightarrow f(x) = y$.

Poznamenejme, že f^{-1} existuje pouze, když f je prostá. Dále platí $H(f^{-1}) = D(f)$, f^{-1} je prostá funkce, $(f^{-1})^{-1} = f$, $(f^{-1} \circ f)(x) = x$ pro každé $x \in D(f)$ a $(f \circ f^{-1})(x) = x$ pro každé $x \in D(f^{-1}) = H(f)$. Grafy funkcí f a f^{-1} jsou (v téže kartézské soustavě souřadnic) navzájem souměrné podly přímky $y = x$.

Kapitolu zakončíme diskusí o jistých „*transformacích grafu funkce*". V podstatě půjde o sestrojení grafu funkce pomocí grafů jiných (známých) funkcí, které se od původní funkce moc „neodlišují". Uvažujeme tedy následujících šest případů. Nechť f je funkce.

- $f_1 : y = -f(x)$. Grafy funkcí f a f_1 jsou symetrické podle osy x.
- $f_2 : y = f(-x)$. Grafy funkcí f a f_2 jsou symetrické podle osy y.

- $f_3 : y = f(x) + b$, $b \in \mathbb{R}$. Posunutí grafu ve směru osy y: nahoru pro $b > 0$, dolů pro $b < 0$.
- $f_4 : y = f(x - a)$, $a \in \mathbb{R}$. Posunutí grafu ve směru osy x: doprava pro $a > 0$, doleva pro $a < 0$.
- $f_5 : y = kf(x)$, $k \in (0, \infty)$. Deformace grafu ve směru osy y: k-násobné „zvětšení“ pro $k > 1$, k-násobné „zmenšení“ pro $k \in (0, 1)$.
- $f_6 : y = f(mx)$, $m \in (0, \infty)$. Deformace grafu ve směru osy x: $1/m$-násobné „zúžení“ pro $m > 1$, $1/m$-násobné „roztažení“ pro $m \in (0, 1)$.

9.4 Literatura

[1] L.E. Garner, Calculus and analytic geometry, Dellen Publ. Comp. 1988.

[2] J. Kuben, P. Šarmanová, Diferenciální počet funkcí jedné proměnné, VŠB TU Ostrava 2006.

[3] V. Novák, Diferenciální počet funkcí jedné reálné proměnné, PdF MU Brno 2004.

[4] K. Rektorys a kol., Přehled užité matematiky I, Prometheus 2002.

Kapitola 10

Elementární funkce

Základními elementárními funkcemi máme na mysli polynomy, funkce racionální, exponenciální, logaritmické, mocninné, goniomentrické, cyklometrické, hyperbolické a hyperbolometrické.

Elementárními funkcemi máme na mysli funkce, které lze vytvořit ze základních elementárních funkcí pomocí konečného počtu operací sčítání, odčítání, násobení, dělení a skládání funkcí.

Někdy také rozlišujeme tzv. *algebraické funkce*, tj. funkce, které lze vytvořit z konstant a z proměnné x konečným počtem algebraických operací (tj. sčítáním, odčítáním, násobením, dělením a umocňováním racionálním exponentem – jsou to funkce $y = f(x)$, které lze vyjádřit pomocí polynomu dvou proměnných $P(x, y) = 0$). Sem tedy patří zejména polynomy a racionální funkce. Algebraické funkce lze dále rozdělit na *racionální funkce* a *iracionální funkce* (iracionální funkce jsou zhruba řečeno funkce obsahující $x^{m/n}$, kde m, n jsou nesoudělná). Funkce, která není algebraická, se nazývá *transcendentní.* Ve výše uvedeném výčtu funkcí máme uvedeny všechny tzv. *elementární transcendentní funkce.* Transcendentní funkce lze rozdělit na nižší a vyšší. *Nižší transcendentní funkce* dostaneme pomocí konečného počtu operací sčítání, odčítání, násobení, dělení a skládání elementárních transcendentních funkcí. Je zřejmé, že jak algebraické funkce, tak i nižší transcendentní funkce patří mezi elementární funkce. Existují však i funkce, které nejsou elementární (definují se např. pomocí integrálů či diferenciálních rovnic, ale i jinak). Takové funkce se nazývají *vyšší transcendentní funkce.*

Poznamenejme, že terminologie týkající se výše uvedeného rozdělení funkcí není v literatuře jednotná.

V tomto základním kurzu se nebudeme zabývat funkcemi byperbolickými, hyperbolometrickými a vyššími transcendentními.

10.1 Polynomy a racionální funkce

Polynomy a racionální funkce patří k nejjednodušším elementárním funkcím.

Nechť $n \in \mathbb{N} \cup \{0\}$, $a_1, a_2, \ldots, a_n \in \mathbb{R}$. Funkce

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad x \in \mathbb{R},$$

se nazývá *polynom* (přesněji, *reálný polynom*; někdy též *mnohočlen*). Čísla $a_0, a_1, \ldots, a_n$ se nazývají *koeficienty polynomu* P. Je-li $a_n \neq 0$, nazývá se a_n *vedoucí koeficient* a číslo n *stupeň polynomu* P (píšeme $\operatorname{st} P = n$).

Poznámka 10.1. (i) Stupeň polynomu je tedy nejvyšší mocnina neznámé s nenulovým koeficientem.

(ii) Je-li $\operatorname{st} P = 1$, pak P je *lineární polynom*, je-li $\operatorname{st} P = 2$, pak P je *kvadratický polynom*, je-li $\operatorname{st} P = 3$, pak P je *kubický polynom*. Podle definice je polynom stupně 0 funkce $P(x) = a_0 \neq 0$ (tj. konstantní nenulová funkce). Funkce $P(x) = 0$, $x \in \mathbb{R}$, je tzv. *nulový polynom*, který nemá přiřazen žádný stupeň.

(iii) Někdy bude účelné uvažovat P též jako zobrazení $P : \mathbb{C} \to \mathbb{C}$, tj. $x \in \mathbb{C}$, $a_0, a_1, \ldots, a_n \in \mathbb{C}$.

Nyní se budeme věnovat otázce nalezení řešení rovnice $P(x) = 0$. Nebudeme hledat pouze reálné, ale i komplexní kořeny.

Číslo $x_0 \in \mathbb{C}$ se nazývá *kořen polynomu* P, jestliže $P(x_0) = 0$.

Tzv. *základní věta algebry říká:* Libovolný polynom (s reálnými nebo komplexními koeficienty) stupně alespoň jedna má v množině komplexních čísel alespoň jeden kořen.

Není těžké ukázat, že každý polynom $P_n(x)$, $\operatorname{st} P = n \geq 1$, lze psát ve tvaru

$$P_n(x) = a_n (x - x_1)^{k_1} (x - x_2)^{k_2} \cdots (x - x_m)^{k_m}, \tag{10.1}$$

kde $x_1, \ldots, x_m$ jsou navzájem různé kořeny polynomu P_n. Číslům $k_1, \ldots, k_m$ se říká *násobnosti kořenů* $x_1, \ldots, x_m$, přičemž $m \leq n$ a $k_1 + \cdots + k_m = n$. Tvaru (10.1) říkáme *rozklad polynomu na součin kořenových činitelů v komplexním oboru.* Lineární polynomy $x - x_i$, $i = 1, \ldots, n$, nazýváme *kořenové činitele* (nebo *kořenové faktory*).

Odtud lze vidět, že každý polynom stupně n má v komplexním oboru právě n kořenů, počítáme-li každý kořen tolikrát, kolik činí jeho násobnost.

Označíme-li $x_1, \dots, x_s$ všechny různé reálné kořeny reálného polynomu $P_n(x)$, $n \geq 1$ s násobnostmi $k_1, \dots, k_s$, a dále, označíme-li $x^2+p_1x+q_1, \dots, x^2+p_rx+q_r$ všechny kvadratické trojčleny odpovídající všem navzájem různým dvojicím komplexně sdružených nereálných kořenů s násobnostmi $l_1, \dots, l_r$, pak dostáváme

$$P_n(x) = a_n(x-x_1)^{k_1} \cdots (x-x_s)^{k_s}(x^2+p_1x+q_1)^{l_1} \cdots (x^2+p_rx+q_r)^{l_r}, \quad (10.2)$$

což je tzv. *rozklad polynomu v reálném oboru* (přesněji *rozklad reálného polynomu na součin ireducibilních (tj. nerozložitelných) činitelů v reálném oboru*).

Rozklady (10.1), (10.2) jsou jednoznačné až na pořadí činitelů.

Obecně je úloha nalezení kořenů obtížný úkol (zejména při vyšších stupních). Pro kořeny kvadratických polynomů existuje dobře známý vzorec. Pro výpočet kořenů polynomů třetího či čtvrtého stupně existují též jisté vztahy – výpočty však již mohou být poměrně složité. Bylo ukázáno, že univerzální vzorec pro výpočet kořenů polynomu pátého a vyššího stupně již v jistém („rozumném“) smyslu neexistuje. Poznamenejme, že často se kořeny hledají pomocí tzv. numerických metod, případně existují další metody pro jisté specifické případy.

Připomeňte si alespoň vzorce pro $(a \pm b)^2, (a \pm b)^3, a^2 - b^2, a^3 \pm b^3$.

Je lehké vidět, že jsou-li P, Q polynomy, jsou $P + Q, P - Q, PQ$ rovněž polynomy. Dělením polynomů však již nemusíme dostat polynom, ale obecnější funkci, kterou nyní zavedeme.

Nechť P, Q jsou nenulové polynomy. Funkce

$$R(x) = \frac{P(x)}{Q(x)}$$

se nazývá *racionální funkce* (nebo *racionální lomená funkce*).

Je zřejmé, že nemusí platit $D(R) = \mathbb{R}$.

Racionální funkce R se nazývá *ryzí* (nebo *ryze lomená*), jestliže $\operatorname{st} P < \operatorname{st} Q$ a *neryzí* (nebo *neryze lomená*), jestliže $\operatorname{st} P \geq \operatorname{st} Q$.

Je-li R neryzí, pak lze provést dělení (příslušný algoritmus je znám ze střední školy) a platí

$$R(x) = \frac{P(x)}{Q(x)} = S(x) + \frac{T(x)}{Q(x)},$$

kde S, T jsou polynomy (T je „zbytek“ po dělení), přičemž T může být nulový. V případě, že T je nenulový, pak platí $\operatorname{st} T < \operatorname{st} Q$.

V budoucnu se naučíme rozkládat racionální funkce na tzv. *parciální zlomky*. Zhruba řečeno: původní („komplikovanou“) racionální funkci nahradíme součtem „jednodušších“ racionálních funkcí. Jak také uvidíme, tento rozklad bude hrát důležitou roli v integrálním počtu, ale i jinde.

10.2 Funkce exponenciální, logaritmické a mocninné

Nejprve připomeňme, že mocninu a^b, která je definována pro $a \in \mathbb{R}$, $a > 0$, a $b \in \mathbb{R}$ můžeme zavést např. takto. Nejprve se zavádí a^n, kde $n \in \mathbb{N}$, jako $a^n = a \cdot a \cdots a$ (činitelů je n). Dále, číslo $x \in \mathbb{R}$, $x > 0$, pro něž platí $x^n = a$, nazýváme n-tou odmocninou z čísla a a značíme symbolem $\sqrt[n]{a}$. Je-li nyní $c \in \mathbb{Q}$, $c = m/n$, $m \in \mathbb{Z}$, $n \in \mathbb{N}$, klademe $a^c = \sqrt[n]{a^m}$. Konečně, je-li $b \in \mathbb{R}$ libovolné, klademe $a^b = \lim_{n\to\infty} a^{c_n}$, kde $\{c_n\}$ je libovolná posloupnost racionálních čísel taková, že $\lim c_n = b$ (lze ukázat, že definice je korektní a vše „dobře funguje“). Pojem limity by měl být znám ze střední školy a my jej budeme v detailech studovat později. Alternativně lze zavést obecnou mocninu jako $a^b = \sup\{a^c : c < b, c \in \mathbb{Q}\}$, kde $a > 1$, $b \in \mathbb{I}$. Je-li $0 < a < 1$, pak se použije infimum. Pro takto definované mocniny platí obyklá početní pravidla a nerovnosti.

Nechť $a \in \mathbb{R}$, $a > 0$. Funkce $f(x) = a^x$, $x \in \mathbb{R}$, se nazývá *exponenciální funkce (o základu a)*.

Případ $a = 1$ je triviální, a proto se omezíme na případ $a \neq 1$. Základní vlastnosti funkce $f(x) = a^x$, $a > 0$, $a \neq 1$, jsou tyto:

- $D(f) = \mathbb{R}$, $H(f) = (0, \infty)$.
- $a > 1 \Rightarrow f$ je rostoucí, $0 < a < 1 \Rightarrow f$ je klesající.
- $x_1, x_2 \in \mathbb{R} \Rightarrow a^{x_1+x_2} = a^{x_1}a^{x_2}$, $a^{x_1-x_2} = a^{x_1}/a^{x_2}$, $(a^{x_1})^{x_2} = a^{x_1x_2}$.

Důležitým speciálním případem je tzv. *přirozená exponenciální funkce* $f(x) = e^x$, kde $e \in \mathbb{I}$ je tzv. *Eulerovo číslo*, $e = \lim_{n\to\infty}(1 + 1/n)^n \doteq 2,718$.

Viděli jsme, že pro $a \neq 1$ je a^x ryze monotonní a tedy prostá. Proto k ní existuje funkce inverzní.

Nechť $a \in \mathbb{R}$, $a > 0$, $a \neq 1$. Inverzní funkce k funkci $f(x) = a^x$ se nazývá *logaritmická funkce o základu* a a značí se $\log_a x$.

Zřejmě tedy $y = \log_a x \Leftrightarrow x = a^y$. Základní vlastnosti funkce $f(x) = \log_a x$ jsou tyto:

- $D(f) = (0, \infty)$, $H(f) = \mathbb{R}$.
- $a > 1 \Rightarrow f$ je rostoucí, $0 < a < 1 \Rightarrow f$ je klesající.
- $x_1, x_2 \in (0, \infty) \Rightarrow \log_a(x_1 x_2) = \log_a x_1 + \log_a x_2$, $\log_a(x_1/x_2) = \log_a x_1 - \log_a x_2$, $x_1 \in (0, \infty)$, $x_2 \in \mathbb{R} \Rightarrow \log_a x_1^{x_2} = x_2 \log_a x_1$.
- $a, b \in \mathbb{R}$, $a > 0$, $b > 0$, $a \neq 1 \neq b \Rightarrow \log_a x = \log_b x / \log_b a$ pro každé $x \in (0, \infty)$, $a^x = b^{x \log_b a}$ pro každé $x \in \mathbb{R}$.

Důležitým speciálním případem je tzv. *přirozená logaritmická funkce* $\ln x = \log_e x$ (značí se též $\lg x$ nebo $\log x$).

Nechť $a \in \mathbb{R}$. Funkce $f(x) = x^a$, $x \in (0, \infty)$, se nazývá *mocninná funkce (s reálným exponentem a)*.

Případ $a = 0$ je nezajímavý, neboť $x^0 = 1$ pro všechna $x \in (0, \infty)$. Základní vlastnosti funkce $f(x) = x^a$, $a \in \mathbb{R}$, $a \neq 0$, jsou tyto:

- $D(f) = (0, \infty)$, $H(f) = (0, \infty)$.
- $a > 0 \Rightarrow f$ je rostoucí, $a < 0 \Rightarrow f$ je klesající.
- $x_1, x_2 \in (0, \infty) \Rightarrow (x_1 x_2)^a = x_1^a x_2^a$, $(x_1/x_2)^a = x_1^a / x_2^a$.

Pro některé speciální hodnoty čísla a je $D(f)$ funkce $f(x) = x^a$ širší než interval $(0, \infty)$ ve shodě s tím, pro které hodnoty $x \in \mathbb{R}$ může být mocnina x^a definována. Zejména platí:

- Pro $a \in \mathbb{N}$ je $D(f) = \mathbb{R}$.
- Pro $a \in \mathbb{Z}$, $a \leq 0$, je $D(f) = (-\infty, 0) \cup (0, \infty)$.
- Pro $a \in \mathbb{Q}$, $c = m/n$, $m \in \mathbb{Z}$, $n \in \mathbb{N}$, kde zlomek m/n je v základním tvaru, přičemž n je liché: v případě $m > 0$ je $D(f) = \mathbb{R}$; v případě $m < 0$ je $D(f) = (-\infty, 0) \cup (0, \infty)$.

Uvědomte si, že pracujeme v $\mathbb{R}$. Jinak bychom s těmito výrazy zacházeli v $\mathbb{C}$.

10.3 Funkce goniometrické a cyklometrické

Goniometrickými funkcemi nazýváme níže definované funkce $\sin x$, $\cos x$, $\operatorname{tg} x$, $\operatorname{cotg} x$. *Cykometrickými funkcemi* nazýváme funkce $\arcsin x$, $\arccos x$, $\operatorname{arctg} x$, $\operatorname{arccotg} x$ (jsou to inverze ke goniometrickým funkcím při příslušném „zúžení“ jejich definičních oborů).

Funkce $\sin x$ a $\cos x$ budeme zavádět jako na střední škole (přičemž však budeme používat zatím ne zcela exaktně zavedenou operaci „nanášení oblouku délky $|x|$ na jednotkovou kružnici“). Později poznáme i jiné možnosti, jak tyto funkce zavést formálně přesně (např. pomocí nekonečných řad, či diferenciálních rovnic).

Nechť A je koncový bod oblouku na jednotkové kružnici, jehož počáteční bod je $(1, 0)$ a jehož délka je $|x|$. Přitom oblouk nanášíme na kružnici v kladném smyslu (proti oběhu hodinových ručiček), je-li $x \geq 0$, resp. v záporném smyslu, je-li $x < 0$. Pak první souřadnici bodu A nazýváme $\cos x$ (tzv. *kosinus*) a druhou souřadnici $\sin x$ (tzv. *sinus*). Dále definujeme $\operatorname{tg} x = \sin x / \cos x$ (tzv. *tangens*) a $\operatorname{cotg} x = \cos x / \sin x$ (tzv. *kotangens*).

Poznamenejme, že číslo π, jež v úvahách o goniometrických funkcích hraje zásadní roli, je polovinou délky jednotkové kružnice. Je známo, že $\pi \in \mathbb{I}$ a je transcendentní, tj. není kořenem žádného polynomu s celočíselnými koeficienty.

Úhly budeme nadále měřit v míře obloukové, nikoliv stupňové. Připomeňme, že úhel $1°$ v míře stupňové je roven úhlu $\pi/180$ v míře obloukové. Obecně úhel n stupňů má obloukovou míru $n\pi/180$.

Základní vlastnosti goniometrických funkcí jsou tyto:

- $D(\sin) = D(\cos) = \mathbb{R}$, $D(\operatorname{tg}) = \mathbb{R} \setminus \{(2k+1)\pi/2 : k \in \mathbb{Z}\}$, $D(\operatorname{cotg}) = \mathbb{R} \setminus \{k\pi : k \in \mathbb{Z}\}$.
- $H(\sin) = H(\cos) = \langle -1, 1 \rangle$, $H(\operatorname{tg}) = H(\operatorname{cotg}) = \mathbb{R}$.
- Funkce $\sin x, \operatorname{tg} x, \operatorname{cotg} x$ jsou liché, funkce $\cos x$ je sudá.
- Funkce $\sin x, \cos x$ jsou 2π-periodické, funkce $\operatorname{tg} x, \operatorname{cotg} x$ jsou π-periodické.

Cykometrické funkce jsou inverzní ke goniometrickým. Protože však inverzní funkci lze setrojit pouze k funkci, která je prostá, je třeba patřičným způsobem „zúžit“ definicční obory příslušných goniometrických funkcí.

Inverzní funkce k funkci sin definované na intervalu $\langle -\pi/2, \pi/2 \rangle$ se značí arcsin (tzv. *arkussinus*). Inverzní funkce k funkci cos definované na intervalu $\langle 0, \pi \rangle$ se značí arccos (tzv. *arkuskosinus*). Inverzní funkce k funkci tg definované na intervalu $(-\pi/2, \pi/2)$ se značí arctg (tzv. *arkustangens*). Inverzní funkce k funkci cotg definované na intervalu $(0, \pi)$ se značí arccotg (tzv. *arkuskotangens*).

Základní vlastnosti cyklometrických funkcí jsou tyto:

- $D(\arcsin) = D(\arccos) = \langle -1, 1 \rangle$, $D(\operatorname{arctg}) = D(\operatorname{arccotg}) = \mathbb{R}$.

- $H(\text{arcsin}) = \langle -\pi/2, \pi/2 \rangle$, $H(\text{arccos}) = \langle 0, \pi \rangle$, $H(\text{arctg}) = (-\pi/2, \pi/2)$, $H(\text{arccotg}) = (0, \pi)$.
- Funkce $\arcsin x$, $\operatorname{arctg} x$ jsou rostoucí. Funkce $\arccos x$, $\operatorname{arccotg} x$ jsou klesající.
- Funkce $\arcsin x$, $\operatorname{arctg} x$ jsou liché.

Existuje řada (důležitých a užitečných) vztahů mezi goniometrickými funkcemi a mezi cyklometrickými funkcemi (např. $\sin^2 x + \cos^2 x = 1$ atd.). S použitím vhodné literatury si přehledným způsobem sepište alespoň ty nejdůležitější identity. Rovněž bude užitečné, pokud si připomenete hodnoty goniometrických a cyklometrických funkcí ve význačných bodech (např. $\sin(\pi/6) = 1/2$ atd.) a vytvoříte si příslušné tabulky.

10.4 Literatura

[1] L.E. Garner, Calculus and analytic geometry, Dellen Publ. Comp. 1988.

[2] J. Kuben, Z. Došlá, Diferenciální počet funkcí jedné proměnné, PřF MU Brno 2003.

[3] J. Kuben, P. Šarmanová, Diferenciální počet funkcí jedné proměnné, VŠB TU Ostrava 2006.

[4] V. Novák, Diferenciální počet funkcí jedné reálné proměnné, PdF MU Brno 2004.

[5] K. Rektorys a kol., Přehled užité matematiky I, Prometheus 2002.