evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Profesní pŚprava uļ itelŢ pŚrodovŊdných oborŢ pro uplatnŊní v konkurenļ ním prostŚedí

CZ.1.07/2.2.00/15.0310

Úvod do studia matematiky

Petr Emanovský

Olomouc 2011

OBSAH

Pśedmluva

Milí mladí přátelé,

Přesto, že se říká, že matematika je jen jedna, způsob výkladu matematiky se může značně lišit. Zatímco na střední škole je kladen důraz na řešení konkrétních úloh, vysokoškolská matematika bývá zpravidla přednášena podle tradičního schématu „Definice – věta – důkaz“. Tento způsob výkladu vám může zpočátku činit jisté potíže. Budete zavaleni spoustou nových abstraktních pojmů, které jsou však nezbytné pro vaše další studium matematických disciplín. K tomu, abyste novým pojmům správně porozuměli, je třeba zodpovědět řadu otázek, absolvovat mnohá cvičení a vyřešit spoustu úloh. Ne nadarmo se říká, že matematický text se nečte, ale „studuje s tužkou v ruce“. Studijní text, který se vám dostává do rukou obsahuje kromě potřebné teorie také otázky a cvičení, na kterých byste si měli vyzkoušet, zda jste jednotlivé pojmy správně pochopili. U některých cvičení vám budou stačit znalosti ze střední školy, některá budete schopni zvládnout až v průběhu vašeho dalšího studia. V každém případě se od vás očekává aktivní přístup při hledání odpovědí na otázky a při provádění cvičení. Pokud budete mít při studiu problémy, neváhejte a snažte se najít odpověď v literatuře, na internetu nebo u svých vyučujících.

Matematika je krásná věda, která však odhalí svou krásu jenom tomu, kdo má dostatek trpělivosti překonat překážky objevující se zejména na počátku jejího studia. Přeji vám, abyste tuto trpělivost v sobě našli a podařilo se vám zažít příjemné pocity z objevování krásy matematiky. Následující studijní text by vám při tom měl pomoci. Byl vytvořen za podpory grantu EU OPVK CZ.1.07/2.2.00/15.0310 „Profesní příprava učitelů přírodovědných oborů pro uplatnění v konkurenčním prostředí“ a měl by sloužit zejména jako podpůrný text vyučovacího předmětu „Úvod do studia matematiky pro každého“, který v rámci tohoto projektu vznikl.

V Olomouci, 2011 Autor

1 Základy matematické logiky

1.1 Formalizovaný matematický jazyk

Cíle
Po prostudování této kapitoly dokážete:

- porozumět rozdílu mezi formalizovaným a živým jazykem,
- pochopit význam formalizovaného jazyka pro přesné vyjadřování v matematice,
- správně chápat a používat základní matematickou symboliku.

Z hodin matematiky si jistě pamatujete, že matematické poučky jsou zpravidla vyjadřovány a zapisovány specifickým (*formalizovaným*) jazykem, odlišným od běžného živého jazyka. Proč matematika potřebuje svůj vlastní jazyk? V zásadě ze dvou hlavních důvodů – kvůli *pŚesnosti* vyjadřování a *zjednodušení* zápisů. Ukažme si to na dvou jednoduchých příkladech:

PŚíklad
Zápis $\forall\ a, b \in R;\ a^2 - b^2 = (a + b)\cdot(a - b)$ není větou českého jazyka, neboť obsahuje speciální symboly, které nepatří do české abecedy. Pokud bychom chtěli tuto rovnost vyjádřit slovně (běžným jazykem), působilo by to dost neohrabaně: „Rozdíl druhých mocnin libovolných dvou reálných čísel je roven součinu součtu a rozdílu těchto dvou čísel.“ Formalizovaný jazyk nám tedy umožňuje jednodušší přehlednější zápis matematických výrazů a tím také usnadňuje práci s výrazy (např. úpravy výrazů).

PŚíklad
Uvažujme větu: „Číslo x je nejmenší přirozené číslo, které není možno charakterizovat pomocí věty českého jazyka zapsané pomocí nejvýše 200 písmen.“ Tato věta je však větou českého jazyka, která je zapsána pomocí méně než 200 písmen a charakterizuje číslo x. Proto x nemůže mít popisovanou vlastnost. Dostáváme tak logický paradox, který je důsledkem nepřesnosti běžného jazyka.

Z uvedených příkladů je vidět, že pro matematiku je účelné budovat přesný (formalizovaný) jazyk. Z hlediska toho, kdo chce studovat určitou matematickou teorii, je velmi důležité dobře znát *symboly* neboli *abecedu*, kterou tato teorie používá a také dobře znát *gramatiku*, tj. pravidla, podle nichž se z abecedy tvoří *slova* (*formule*). Symboly používané v matematických zápisech jsou dvojího druhu – *konstanty* a *proměnné*. Konstantou rozumíme každý jazykový výraz, který má jednoznačně určený smysl. Proměnnou rozumíme jazykový výraz, který sám nemá smysl, ale určuje místo, na které je možné za něj dosazovat konstanty z daného oboru proměnnosti.

Otázky

1. Proč matematika potřebuje vlastní formalizovaný jazyk?
2. Co rozumíme formulí matematické teorie?
3. Co potřebujeme znát, abychom mohli tvořit formule určité matematické teorie?

Cviļení

1) Přečtěte správně následující formule:
   a) $\forall\ a, b \in R;\ a^3 - b^3 = (a - b)\cdot(a^2 + ab + b^2);$
   b) $\exists\ n \in N;\ n^2 = -1;$
   c) $\exists\ e \in G\ \forall\ a \in G;\ e \bullet a = a \bullet e = a;$
   d) $\forall a \in G\ \exists\ e \in G;\ e \bullet a = a \bullet e = a;$
   e) $A = (0, 4);$
   f) $B = \{1, 2, 3\};$
   g) $M = \{n \in N\ ;\ n < 4\};$
   h) $K = \{x \in R\ ;\ f(x) = 3\};$
   i) $T = \{(x, y) \in A \times B;\ x = y + 1\};$
   j) $S = \{X \in P(A);\ X \subseteq M\};$
   k) $\forall x \in R(x \neq 0 \Rightarrow x^2 > 0);$
   l) $\exists x \in R(x > 0 \wedge x < 3);$
   m) $\forall a \in N(6 \mid a \Leftrightarrow (3 \mid a \wedge 2 \mid a));$
   n) $W \subseteq \subseteq V;$
   o) [illegible] $\in$ [illegible], $\cdots$ [illegible].

2) Zapište pomocí matematických symbolů:
   a) A je množina všech přirozených čísel dělitelných pěti.
   b) Množina B je podmnožinou průniku množin C a D.
   c) Pro každé reálné číslo x platí, že jeho druhá mocnina zvětšená o jedničku je číslo kladné.
   d) Sjednocení množin je komutativní operace.
   e) Průnik množin je asociativní operace.
   f) Průnik množin je distributivní vzhledem ke sjednocení.
   g) Jestliže přirozené číslo x je větší než 3, pak existuje přirozené číslo y, které je menší než x.
   h) Kartézský součin množin A a B je množina všech uspořádaných dvojic takových, že jejich první složka patří do množiny A a druhá složka do množiny B.
   i) Uspořádaná dvojice vytvořená z přirozených čísel x a y patří relaci R právě tehdy, když 3 dělí $x+y$.
   j) Zobrazení f přiřazuje každému reálnému číslu jeho druhou mocninu zmenšenou o 5.
   k) Operace $\bullet$ definovaná na množině M je komutativní.
   l) Operace $\bullet$ definovaná na množině M je asociativní.
   m) Operace $\bullet$ definovaná na množině M je distributivní vzhledem k operaci $*$ definované na množině M.
   n) Vektor [illegible] $\in R^n$ je lineární kombinací vektorů [illegible], …, [illegible] $\in R^n$.
   o) Lineární obal množiny M, která je podmnožinou vektorového prostoru V, je roven množině všech lineárních kombinací vektorů z M.
   p) W je podprostorem vektorového prostoru V.
   q) Matice B vznikla z matice $A =$ [illegible] vynásobením jejího i-tého řádku číslem c.
   r) Determinant matice B vznikl vynásobením k-tého sloupce determinantu matice $A =$ [illegible] číslem c.
   s) Dimenze prostoru W je rovna dimenzi průniku prostorů S a T.
   t) Hodnost matice A je větší než hodnost matice B.
   u) Jádro homomorfismu f je jednoprvkové.

v) Vektor [illegible] leží v podprostoru generovaném vektory [illegible], …, [illegible].

3) Rozhodněte, zda následující zápisy dávají smysl, příp. je vhodně upravte:
   a) $M = \{n \in N;\ n\}$;
   b) $\exists y \in R(x > 0 \wedge x < 3)$;
   c) [illegible] = [illegible];
   d) $detA$ = [illegible];
   e) $A = \{(x, y) \in N^3;\ x < y\}$;
   f) $f\colon\ R^n \to R^n,\ f((x_1,$ é $, x_n)) = x_1 +$ é $+ x_n$;
   g) $g\colon\ R^3 \to R^3,\ g((x, y, z)) = (x - y, x - 3z)$;
   h) c_1 [illegible] + … + c_k [illegible] = 0;
   i) $dimV$ = { [illegible], …, [illegible] }.

1.2 Výroky, výrokové formule, výrokové formy

Cíle

Po prostudování této kapitoly dokážete:

- porozumět obsahu pojmů výrok, výroková formule, výroková forma,
- pracovat se základními logickými spojkami a vyhodnocovat tabulky pravdivostních hodnot výrokových formulí,
- určovat obory pravdivosti výrokových forem,
- tvořit kvantifikované výroky a jejich negace.

Výrokem rozumíme každé sdělení, o němž má smysl uvažovat, zda je pravdivé nebo nepravdivé, přičemž může nastat právě jedna z těchto dvou možností.
Zkusme se zamyslet nad tím, která z následujících sdělení jsou výroky, případně jaká je jejich pravdivost:
A: Číslo 2 je větší než nula.
B: $2^2 = 5$.
C: Velryba není savec.
D: Ve vesmíru existuje život i mimo Zemi.
E: $a^2 - b^2 = (a + b)\cdot(a - b)$.
F: $\exists\ a, b, c \in N;\ c^2 = a^2 + b^2$.
G: $\exists\ a, b, c, n \in N,\ n > 2;\ c^n = a^n + b^n$.
H: Jestliže velryba není savec, pak $2^2 = 5$.

Zřejmě A je pravdivý výrok, zatímco B a C jsou výroky nepravdivé. Případ D je výrokem ve smyslu naší definice, v současné době ovšem neznáme jeho pravdivost (jde o tzv. *hypotézu*). E není výrokem, pokud nevíme nic bližšího o proměnných a, b. V této kapitole se dozvíme, že se jedná o tzv. *výrokovou formu*, z níž lze vytvořit výrok pomocí *kvantifikátorŢ* (např. $\forall\ a, b \in R;\ a^2 - b^2 = (a + b)\cdot(a - b)$ je výrok pravdivý). F je výrok pravdivý, např. $5^2 = 3^2 + 4^2$. Případ G odpovídá negaci tzv. Velké Fermatovy věty, která byla po dobu více než 350 let hypotézou odolávající pokusům o důkaz či vyvrácení. Důkaz této věty byl podán až koncem 20. století. G je tedy výrok nepravdivý. V případě H se jedná o výrok, dokonce pravdivý.
Výrok H je tzv. *sloģený výrok*, neboť jej lze rozdělit na dva samostatné výroky (v tomto případě výroky C a B). Ostatní výroky z našeho příkladu tuto vlastnost nemají. Takovým výrokům říkáme *atomární výroky*.

V matematice často řešíme otázku, jak závisí pravdivost složeného výroku na pravdivostech jeho jednotlivých atomárních výroků. Touto problematikou se zabývá tzv. *výroková logika*. Pro naše potřeby bude stačit znalost základních *výrokových spojek* (*negace*, *konjunkce*, *disjunkce*, *implikace*, *ekvivalence*), s nimiž jste se již setkali na střední škole. Pro zjednodušení zápisu zavádíme formalizovaný jazyk, jehož součástí je abeceda a gramatika (viz kapitola 1.1). Konstantami této abecedy jsou symboly pro výrokové spojky ($\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$) a pomocné symboly (závorky). Proměnnými jsou symboly zastupující konkrétní výroky (A, B, C, …), tzv. *výrokové proměnné*. Z uvedených symbolů pak skládáme pomocí jistých pravidel (gramatiky) tzv. *výrokové formule* (neplést s výrokovými formami!). Pro jednoduchost však zpravidla nedosazujeme do výrokových formulí za výrokové proměnné výroky, ale pouze jejich *pravdivostní hodnoty* (1 pro pravdivý výrok, 0 pro nepravdivý výrok) a vše zapisujeme do přehledné tabulky. Z hlediska matematické logiky mají velký význam výrokové formule, které mají vždy pravdivostní hodnotu 1. Říkáme jim *tautologie* a jsou to vlastně logické zákony, které lze využít např. při důkazech matematických vět. Naopak formule, jejichž pravdivostní hodnota je vždy 0, nazýváme *kontradikce*. *Splnitelnou formulí* nazveme takovou formuli, která nabývá pravdivostní hodnoty 1 alespoň pro jedno dosazení za její výrokové proměnné. Tautologie je tedy speciálním případem splnitelné formule.
Z předchozího výkladu je zřejmé, že výroková logika pracuje pouze s pravdivostními hodnotami výroků a nezajímá se o jejich vnitřní stavbu. Touto problematikou se zabývá tzv. *predikátová logika*. Základním pojmem predikátové logiky je pojem *výroková forma*. Výrokovou formou rozumíme takové sdělení, které obsahuje proměnné a které se stane výrokem po dosazení konstant z *oborů proměnnosti* za všechny proměnné, nebo vázáním všech proměnných pomocí kvantifikátorů.

Příklad
Následující sdělení jsou výrokovými formami:

1. $V(x)$: x je dělitelné třemi,
2. $W(x)$: $x < 6$,
3. $U(x)$: [illegible]/[illegible] < 5,
4. $S(x, y)$: x dělí y.

Z uvedených výrokových forem lze tvořit výroky dosazením za proměnné z oborů proměnnosti nebo vázáním proměnných kvantifikátory. V případě výrokové formy $V(x)$ bychom za obor proměnnosti mohli vzít množinu všech přirozených čísel. Po dosazení jakéhokoliv přirozeného čísla za x dostaneme výrok. Pravdivý výrok dostaneme pouze tehdy, dosadíme-li za x přirozené číslo dělitelné třemi. Např. symbolem $V(12)$ označujeme pravdivý výrok „12 je dělitelné třemi“. *Obor pravdivosti* výrokové formy $V(x)$ je tedy množina $P_1 = \{3, 6, 9, \dots\}$. Podobně, jestliže pro $W(x)$ vezmeme za obor proměnnosti množinu všech reálných čísel, bude oborem pravdivosti $P_2 = (-\infty, 6)$. V případě $U(x)$ je třeba si uvědomit, že tato výroková forma nemá smysl pro $x = 2$. Za obor proměnnosti tedy můžeme vzít množinu $(-\infty, 2) \cup (2,\infty)$ a oborem pravdivosti bude $P_3 = (-\infty, 2) \cup ($[illegible]/[illegible]$, \infty)$. Výroková forma $S(x, y)$ obsahuje dvě proměnné a jejím oborem proměnnosti by mohla být množina všech uspořádaných dvojic (x, y) vytvořených z přirozených čísel (tzv. kartézský součin $N \times N$). Oborem pravdivosti pak bude množina všech dvojic (x, y) z $N \times N$, pro něž platí, že x dělí y. Do této množiny patří např. dvojice (1, 2), (2, 4), (5, 10), ale nepatří do ní např. dvojice (3, 5) nebo (10, 5).
Výroky lze vytvořit z výrokových forem rovněž *vázáním proměnných* (všech!) pomocí *kvantifikátorů*. Např. zápis $\forall x(V(x))$ čteme „Pro každé x platí $V(x)$“ neboli „Pro každé x platí: x je dělitelné třemi“. Toto sdělení je již výrokem (tzv. *obecný výrok* příslušný k výrokové

formě $V(x)$), a to výrokem nepravdivým. Symbol $\forall x$ nazýváme *obecný kvantifikátor*. Podobně zápis $\exists x(V(x))$ čteme „Existuje alespoň jedno x takové, že platí $V(x)$“ neboli „Existuje alespoň jedno x dělitelné třemi“. Toto sdělení je výrokem (tzv. *existenční výrok* příslušný k výrokové formě $V(x)$), a to výrokem pravdivým. Symbol $\exists x$ nazýváme *existenční kvantifikátor*. Poznamenejme, že např. $\forall x(S(x, y))$ není výrok, neboť kvantifikátorem je vázána pouze proměnná x, zatímco proměnná y vázána není (tzv. *volná proměnná*).

Otázky

1. Co je to výrok?
2. Co je hypotéza?
3. Co je složený výrok?
4. Co rozumíme výrokovou formou?
5. Co je volná proměnná?
6. Co je vázaná proměnná?
7. Jakým způsobem lze z výrokové formy vytvořit výrok?
8. Co rozumíme výrokovou formulí?
9. Co je to tautologie?
10. Co rozumíme kontradikcí?
11. Co rozumíme splnitelnou formulí?

Cvičení

1) Rozhodněte, ve kterém z následujících případů se jedná o výrok, případně určete jeho pravdivost:
   a) Venku prší.
   b) Kolik je hodin?
   c) Půjč mi 100 korun!
   d) Praha je hlavní město Československa.
   e) $x + 1 = 0$.
   f) Pavel navštívil Paříž i Londýn.
   g) Bude otevřená restaurace U Huberta nebo Bristol.
   h) Večer půjdu do kina nebo do divadla.
   i) Jestliže dnes dokončím článek, půjdu večer na procházku.
   j) Jestliže 1 + 1 = 2, pak Olomouc leží na Hané.
   k) Jestliže 1 + 1 = 2, pak Olomouc leží v Africe.
   l) Jestliže 1 + 1 = 3, pak Olomouc leží v Africe.
   m) Jestliže 1 + 1 = 3, pak Olomouc leží na Hané.
   n) 1 + 1 = 3 právě tehdy, když Olomouc leží v Africe.
   o) 1 + 1 = 2 právě tehdy, když Olomouc leží v Africe.
   p) 1 + 1 = 2 právě tehdy, když Olomouc leží na Hané.
   q) 1 + 1 = 3 právě tehdy, když Olomouc leží na Hané.
   r) $\forall x \in N\ (x < 3)$.
   s) $\exists x \in N\ (x < 3)$.
   t) $\exists x \in N\ (x + y = 1)$.
   u) $\forall x \in N\ \exists\ x \in N\ (x + y = 1)$.
   v) $\exists x \in N\ \forall x \in N\ (x + y = 1)$.

2) Rozhodněte, které výroky z předcházejícího cvičení jsou atomární a které složené.

3) Negujte následující výroky, příp. se zamyslete nad jejich pravdivostí:
   a) Dnes nepřijde ani Petr ani Pavel.
   b) Venku je zima a nesvítí slunce.
   c) Udělám to já nebo Tomáš.
   d) Každá růže má trní.
   e) Žádné auto není modré nebo aspoň jedno auto je žluté.
   f) Žádný člověk není bez chyby a každý člověk se může mýlit.
   g) Jestliže se budu učit, udělám zkoušku z algebry.
   h) Budu-li mít volno, půjdu do kina nebo do divadla.
   i) Žádná kulička ležící na tomto stole není modrá.
   j) Alespoň jedno celé číslo je sudé a žádné celé číslo není liché.
   k) Pro všechna kladná reálná čísla r, s platí $r < r \cdot s$.
   l) Existují celá čísla $t_1, \ldots, t_n$, z nichž alespoň jedno je různé od nuly taková, že $t_1 + \ldots + t_n = 0$.
   m) Pro libovolná přirozená čísla $a_1, \ldots, a_n$, kde $n \geq 5$ a alespoň jedno z těchto čísel je větší než 5, platí $a_1 + \ldots + a_n \geq 10$.
   n) Existují ryze imaginární čísla z_1, z_2, z_3, jejichž součin je číslo reálné.
   o) $\forall x \in R(x \neq 0 \Rightarrow x^2 > 0)$.
   p) $\exists x \in R(x > 0 \wedge x < 3)$.
   q) $\forall a \in N(6 | a \Leftrightarrow (3 | a \wedge 2 | a))$.
   r) $\exists x \in N \ \forall x \in N(y^x > y)$.
   s) $\forall x \in N \ \exists \ x \in N \ (y^x = y)$.
   t) $\exists x \in N \ \exists \ x \in N \ ((x + y)^2 = 2(x + y))$.
   u) $\forall a \in N \ \forall b \in N \ (a < b \Rightarrow \exists x \in N \ (a < x \wedge x < b))$.

4) Rozhodněte, které z následujících výrazů jsou formule výrokové logiky:
   a) $(A \neg B) \Rightarrow (C \Leftrightarrow D)$,
   b) $(\wedge C \vee E) \Rightarrow \neg B$,
   c) $\neg (A \Rightarrow B) \Leftrightarrow (A \wedge \neg B)$,
   d) $(((A \Rightarrow B) \wedge (\neg B \Leftrightarrow D))$,
   e) $\neg (A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$,
   f) $(X \Rightarrow (Y \Leftrightarrow Z)) \Leftrightarrow ((X \Rightarrow Y) \Leftrightarrow (X \Rightarrow Z))$,
   g) $\neg (A \Leftrightarrow B) \Leftrightarrow ((A \wedge \neg B) \vee (\neg A \wedge B))$.

5) Vyplňte tabulky pravdivostních hodnot pro formule z předchozího příkladu a rozhodněte, které z nich jsou tautologie, případně splnitelné formule nebo kontradikce.

6) Ověřte, že jsou následující výrokové formule tautologie:
   a) $A \vee \neg A$ (zákon vyloučení třetího),
   b) $\neg(A \wedge \neg A)$ (zákon sporu),
   c) $\neg(\neg A) \Leftrightarrow A$ (zákon sporu),
   d) $(A \wedge (B \wedge C)) \Leftrightarrow ((A \wedge B) \wedge C)$ (zákon asociativní pro konjunkci),
   e) $(A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C)$ (zákon asociativní pro disjunkci),
   f) $(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$ (distributivnost konjunkce vzhledem k disjunkci),
   g) $(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$ (distributivnost disjunkce vzhledem ke konjunkci),
   h) $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ (tranzitivita implikace),
   i) $\neg(A \Rightarrow B) \Leftrightarrow (A \wedge \neg B)$,

j) $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$.

7) Zapište ve tvaru $\{x \in M ; V(x)\}$ následující množiny:
   a) množinu všech jednociferných násobků čísla 3,
   b) množinu všech třetích komplexních odmocnin z jedné,
   c) množinu všech reálných řešení rovnice $x^2 - x - 6 = 0$,
   d) množinu všech přirozených dělitelů čísla 24,
   e) množinu všech uspořádaných dvojic přirozených čísel takových, že první složka v každé dvojici je větší než druhá složka,
   f) množinu všech reálných čísel, která se v zobrazení f zobrazí na nulu,
   g) množinu všech obrazů zobrazení g: $A \to B$,
   h) množinu všech prvků grupoidu G s neutrálním prvkem n, k nimž existuje prvek symetrický,
   i) množinu všech netriviálních dělitelů nuly okruhu $(A, +, \cdot)$,
   j) množinu všech regulárních matic stupně n,
   k) množinu všech lineárních kombinací vektorů z podmnožiny M vektorového prostoru V,
   l) průnik podprostorů W_1 a W_2 vektorového prostoru V,
   m) součet podprostorů W_1 a W_2 vektorového prostoru V,
   n) jádro homomorfismu f vektorového prostoru V do vektorového prostoru V'.

8) Uveďte příklad množiny M a výrokové formy $V(x)$ tak, aby
   a) $\{x \in M ; V(x)\}$ byla prázdná množina,
   b) $\{x \in M ; V(x)\}$ byla celá množina M.

9) Uveďte příklad množiny M a dvou různých výrokových forem $V(x)$ a $W(x)$ tak, aby platilo $\{x \in M ; V(x)\} = \{x \in M ; W(x)\}$.

10) Ověřte, že výroková formule $\neg (A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$ je tautologie (tzv. de Morganův zákon) a zformulujte pomocí této tautologie následující výroky, popř. výrokové formy v jiném, ekvivalentním tvaru:
   a) Není pravda, že číslo π je racionální a kladné.
   b) Není pravda, že Albert Einstein byl Angličan a žil v 15. století.
   c) Není pravda, že čtyřúhelník $ABCD$ je kosočtverec nebo lichoběžník.
   d) Není pravda, že přirozené číslo k je dělitelné dvěma nebo třemi.

11) Ověřte, že výroková formule $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ je tautologie (tzv. zákon transpozice) a zformulujte pomocí této tautologie následující výroky, popř. výrokové formy v jiném, ekvivalentním tvaru:
   a) Jestliže čtyřúhelník $ABCD$ je rovnoběžník, pak se jeho úhlopříčky navzájem půlí.
   b) Jestliže je přirozené číslo x dělitelné dvěma a třemi, pak je dělitelné šesti.
   c) Jestliže je přirozené číslo x dělitelné dvěma a čtyřmi, pak je dělitelné osmi.
   d) Jestliže nebudu moci přijet, pošlu telegram.
   e) Jestliže má pacient chřipku, pak má zvýšenou teplotu.

12) Ověřte, že výroková formule $(A \vee B) \Leftrightarrow (\neg A \Rightarrow B)$ je tautologie a zformulujte pomocí této tautologie následující výroky, popř. výrokové formy v jiném, ekvivalentním tvaru:
   a) Řešení rovnice $x + 4 = 5$ je kladné nebo záporné.
   b) Zítra přijdu nebo zatelefonuji.
   c) Přijedu vlakem nebo autobusem.

d) V tomto bytě je ústřední nebo etážové topení.
e) $a \geq 10$.

13) Na základě výrokové logiky ověřte, zda následující úsudek je správný. Viníkem je Petr nebo Pavel. Je-li viníkem Petr, pak Pavel nebyl v 11 hodin na místě činu. Je-li viníkem Pavel, pak je jasný motiv činu. Tedy, jestliže byl Pavel v 11 hodin na místě činu, pak je jasný motiv činu.

14) Na ostrově žijí dva kmeny – Praváci, kteří mluví vždy pravdu a Kecalové, kteří vždy lžou. Cestovatel potkal domorodce a zeptal se ho, kdo je. Když uslyšel, že je Pravák, najal ho do služby jako průvodce. Spolu potkali jiného domorodce a cestovatel poslal svého průvodce, aby se tohoto domorodce zeptal, kdo je. Průvodce se vrátil a řekl, že domorodec tvrdí, že je Pravák. Byl průvodce Pravák nebo Kecal?

2 Množiny, relace, zobrazení

2.1 Základní poznatky o množinách

Cíle

Po prostudování této kapitoly dokážete:

- porozumět obsahu pojmu množina,
- správně používat množinovou terminologii a symboliku,
- provádět základní množinové operace.

Pojem *množina* je jedním ze základních pojmů současné matematiky. Pro naše potřeby vystačíme s intuitivní představou množiny jakožto souboru jakýchkoliv objektů (*prvků*). Množiny označujeme zpravidla velkými písmeny a jejich prvky malými písmeny. Zápis $x \in A$ čteme „x je prvkem A“ a zápis $x \notin A$ znamená „x není prvkem A“. Množiny, které obsahují konečný počet prvků, se nazývají *konečné*, ostatním říkáme *nekonečné*. Uvažujeme i tzv. *prázdnou množinu*, která neobsahuje žádné prvky. Prázdnou množinu značíme symbolem $\emptyset$. Konečnou množinu lze zadat *výčtem prvků*, tj. vypíšeme všechny její prvky do složené závorky, např. $B = \{a, b, c\}$. Jiný způsob určení množiny je pomocí *charakteristické vlastnosti*. Je-li $V(x)$ výroková forma o jedné proměnné x a P obor její proměnnosti, pak $A = \{x \in P;\ V(x)\}$ označuje množinu všech prvků $a \in P$, pro něž je $V(a)$ pravdivým výrokem. Připomeňme stručně základní operace s množinami, s nimiž jste se setkali již na střední škole. *Průnikem množin* A a B rozumíme množinu $A \cap B = \{x;\ x \in A \wedge x \in B\}$. *Sjednocením množin* A a B rozumíme množinu $A \cup B = \{x;\ x \in A \vee x \in B\}$. *Rozdílem množin* A a B rozumíme množinu $A \setminus B = \{x;\ x \in A \wedge x \notin B\}$. Dále říkáme, že množina A je *podmnožinou* množiny B (píšeme $A \subseteq B$), jestliže $\forall x (x \in A \Rightarrow x \in B)$. Říkáme, že A je *vlastní podmnožinou* množiny B (značíme $A \subset B$), jestliže $A \subseteq B$ a $A \neq B$. Řekneme, že množina A *se rovná* množině B (píšeme $A = B$), jestliže $\forall x (x \in A \Leftrightarrow x \in B)$, tj. $A \subseteq B \wedge B \subseteq A$. Při práci s množinami je výhodné využívat jejich grafického vyjádření pomocí *Vennových diagramů*, které byste měli rovněž znát ze střední školy.

Otázky

1. Co je to množina?
2. Jakým způsobem může být množina zadána?
3. Co rozumíme průnikem množin?
4. Jaké vlastnosti má operace průnik množin?
5. Co rozumíme sjednocením množin?
6. Jaké vlastnosti má operace sjednocení množin?
7. Co rozumíme rozdílem množin?
8. Jaké vlastnosti má operace rozdíl množin?
9. Kdy řekneme, že množina A je podmnožinou množiny B?
10. Kdy řekneme, že množina A je vlastní podmnožinou množiny B?
11. Kdy řekneme, že množina A se rovná množině B?

Cviļení

1) Pokud je to možné, zadejte následující množiny výčtem prvků, příp. jiným způsobem:
   a) $P = \{x \in R;\ x^2 - x - 6 = 0\}$,
   b) $D = \{x \in N;\ x^2 + 1 = 0\}$,
   c) $C = \{x \in N;\ x \mid 12\}$,
   d) $B = \{x \in N;\ 24 < x \leq 25\}$,
   e) $E = \{x \in R;\ 24 < x \leq 25\}$,
   f) $F = \{x \in N;\ (2 < x \leq 5) \wedge x \mid 12\}$,
   g) $G = \{x \in R;\ (2 < x \leq 5) \vee x \geq 12\}$,
   h) $H = \{x \in R;\ (2 < x \leq 5) \wedge x \geq 12\}$,
   i) $I = \{x \in Q;\ (2 < x \leq 5) \vee x \geq 12\}$,
   j) $A = \{x \in Q;\ (2 < x \leq 5) \wedge x \geq 12\}$,
   k) $R = \{(x, y) \in A^2;\ x \mid y \ \wedge\ 1 < x < y\}$, kde $A = \{1, 2, 3, 4\}$,
   l) M je průnik všech podprostorů vektorového prostoru V.

2) Zadejte následující množiny charakteristickou vlastností:
   a) $A = \{1, 2, 4\}$,
   b) S je množina všech sudých celých čísel,
   c) L je množina všech lichých celých čísel,
   d) $B = \langle -5, 2)$,
   e) $E = \emptyset$,
   f) $F = (-\infty, 2) \cup (2, \infty)$,
   g) $R_1 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$,
   h) $C = \{2, 5\}$,
   i) $D = \{\emptyset, \{2\}, \{5\}, \{2, 5\}\}$,
   j) $W = \{$⍰$\}$, kde ⍰ je nulový vektor vektorového prostoru V.

3) Určete počet prvků následujících množin:
   a) $P = \{x \in R;\ x^2 - x - 6 = 0\}$,
   b) $D = \{x \in N;\ x^2 + 1 = 0\}$,
   c) $A = (-\infty, 2)$;
   d) $B = \{(-\infty, 2)\}$;
   e) $C = \emptyset$;

f) $E = \{\emptyset\}$;
g) $F = \{\{\emptyset\}\}$;
h) $H = \{\{\emptyset\}, 1, R, \{1, 2, 3\}\}$.

4) Znázorněte pomocí Vennových diagramů následující situace:
a) Každý čtverec je rovnoběžník, ale některé rovnoběžníky nejsou čtverce.
b) Každé přirozené číslo, které je dělitelné čtyřmi, je dělitelné dvěma.
c) Některý trojúhelník není ani pravoúhlý, ani rovnoramenný.
d) Každé přirozené číslo, které je dělitelné šesti, je dělitelné dvěma a třemi, a každé přirozené číslo, které je dělitelné dvěma a třemi, je dělitelné šesti.

5) Uvažujme množinu F všech pracovníků jisté firmy a v ní tři podmnožiny: M je podmnožina všech pracovníků mladších 30 let, K je podmnožina všech kvalifikovaných pracovníků a V je podmnožina všech vedoucích pracovníků. Znázorněte pomocí Vennových diagramů následující situace:
a) Každý vedoucí pracovník mladší než 30 let má potřebnou kvalifikaci.
b) Někteří vedoucí pracovníci, jimž je aspoň 30 let, nemají potřebnou kvalifikaci.
c) Každý kvalifikovaný pracovník je na vedoucím místě nebo mu ještě není 30 let.
d) Někteří vedoucí pracovníci s kvalifikací jsou mladší než 30 let.
e) Někteří pracovníci mladší než 30 let nejsou na vedoucím místě (o jejich kvalifikaci nic nevíme).
f) Každý pracovník firmy je mladší než 30 let nebo je na vedoucím místě a každý pracovník mladší než 30 let má potřebnou kvalifikaci.

6) Pomocí Vennových diagramů rozhodněte o správnosti následujících logických úsudků:

a) Každá ryba umí plavat.
Každý úhoř je ryba.
___
Každý úhoř umí plavat.

b) Žádný student není bohatý.
Každý student umí číst.
___
Někteří lidé, kteří umějí číst, nejsou bohatí.

c) Žádný zloděj není poctivý.
Někteří nepoctiví lidé jsou potrestáni.
___
Někteří zloději jsou potrestáni.

d) Všem žertům se lidé smějí.
Žádný z mých referátů není míněn žertem.
___
Žádnému z mých referátů se lidé nesmějí.

e) Někteří kuřáci jsou nemocní.
Někteří z mých příbuzných kouří.
___
Někteří z mých příbuzných jsou nemocní.

f) Všechna nebeská tělesa obíhají kolem Země.

Slunce je nebeské těleso.

Slunce obíhá kolem Země.

g) Kdo se dobře učil, stal se váženým člověkem.
Nejsem vážený člověk.

Neučil jsem se dobře.

h) Kdo se dobře učil, stal se váženým člověkem.
Jsem vážený člověk.

Učil jsem se dobře.

2.2 Relace a zobrazení

Cíle

Po prostudování této kapitoly dokážete:

- porozumět obsahu pojmů binární relace na množině a zobrazení množiny,
- správně používat příslušnou terminologii a symboliku,
- samostatně určovat základní vlastnosti daných relací a zobrazení,
- porozumět obsahu a vzájemnému vztahu pojmů relace ekvivalence a rozklad množiny,
- porozumět obsahu pojmu relace uspořádání.

Jsou-li $M_1, M_2, \cdots, M_n$ neprázdné množiny, pak množinu $M_1 \times M_2 \times \cdots \times M_n$ obsahující všechny uspořádané n-tice $(m_1, m_2, ..., m_n)$, kde $m_i \in M_i$, $i = 1, 2, ..., n$ nazýváme <u>*kartézským součinem množin*</u> $M_1, M_2, \cdots, M_n$. V případě, že $M_1 = M_2 = \cdots = M_n = M$, mluvíme o <u>*kartézské mocnině množiny*</u> M, kterou značíme M^n. Pro $n = 0$ definujeme $M^0 = \{\emptyset\}$.

Libovolnou podmnožinu R kartézského součinu M^n nazýváme <u>*n-ární relací na množině M*</u>. Pro $n = 2$ hovoříme speciálně o <u>*binární relaci na množině M*</u>.

Poznámka: Pro binární relaci používáme někdy místo zápisu $(a, b) \in R$ také zápis aRb. Např. pro relaci „≤“ je obvyklejší psát $a \leq b$ než $(a, b) \in \leq$.

Definice 2.2.1 Nechť R je binární relace na množině M. Říkáme, že

a) R je <u>*rexlexivní*</u> na M, jestliže $\forall a \in M$ platí $(a, a) \in R$,

b) R je <u>*antireflexivní*</u> na M, jestliže $\forall a \in M$ platí $(a, a) \notin R$,

c) R je <u>*symetrická*</u> na M, jestliže $\forall a, b \in M$ platí $(a, b) \in R$ implikuje $(b, a) \in R$,

d) R je <u>*tranzitivní*</u> na M, jestliže $\forall a, b, c \in M$ platí $(a, b) \in R$, $(b, c) \in R$ implikuje $(a, c) \in R$,

e) R je <u>*antisymetrická*</u> na M, jestliže $\forall a, b \in M$ platí $(a, b) \in R$, $(b, a) \in R$ implikuje $a = b$,

f) R je <u>*konektivní*</u> (<u>*souvislá*</u>) na M, jestliže $\forall a, b \in M$ platí $(a, b) \in R$ nebo $(b, a) \in R$,

Definice 2.2.2 Binární relace „$\leq$“ na množině M, která je reflexivní a tranzitivní se nazývá <u>*kvaziuspoŚádání*</u> na M. Množina M, na níž je definováno kvaziuspořádání „$\leq$“ se nazývá <u>*kvaziuspoŚádaná*</u> a značí se (M, $\leq$). Kvaziuspořádaná množina (M, $\leq$) taková, že relace „$\leq$“ je antisymetrická, se nazývá <u>*uspoŚádaná*</u> a relace „$\leq$“ se v tomto případě nazývá <u>*uspoŚádání*</u> na M. Je-li uspořádání navíc konektivní, hovoříme o <u>*lineárním uspoŚádání*</u> a příslušnou uspořádanou množinu v tomto případě nazýváme <u>*lineárnD uspoŚádanou mnoǵinou*</u> nebo též <u>*ŚetDcem*</u>.

Definice 2.2.3 <u>*Relací ekvivalence*</u> (stručně <u>*ekvivalencí*</u>) na množině M rozumíme každou binární relaci na M, která je reflexivní, symetrická a tranzitivní.

Poznámka 2.2.1 Každá relace ekvivalence R definovaná na množině M vytváří tzv. <u>*rozklad mnoǵiny*</u> M, tj. systém $\{M_i,\ i \in I\}$ neprázdných podmnožin množiny M, pro něž platí :

1) $\bigcup_{i \in I} M_i = M$,

2) Jestliže $i \neq j$, pak $M_i \cap M_j = \emptyset$

Označme $[x]_R = \{y \in M,\ yRx\}$. Systém $\{M_i,\ i \in I\}$ neprázdných podmnožin množiny M vytvoříme pomocí relace R na základě podmínky : $\forall\ x, y \in M$: $[x]_R = [y]_R \Leftrightarrow xRy$.

Definici binární relace na množině lze rozšířit tak, že uvažujeme binární relaci mezi dvěma (obecně různými) množinami A a B. <u>*Binární relací mezi mnoǵinami A* a *B*</u> (někdy též <u>*korespondencí mezi mnoǵinami A* a *B*</u>) rozumíme každou podmnožinu f kartézského součinu AxB. Pro binární relaci f mezi množinami A a B označme

Dom$f = \{x \in A,\ \exists y \in B$ tak, že $(x, y) \in f\}$ („domain“- <u>*definiǰní obor korespondence f*</u>),

Im$f = \{\ y \in B,\ \exists x \in A$ tak, že $(x, y) \in f\}$ („image“ – <u>*obor hodnot korespondence f*</u>).

Definice 2.2.4 Je-li $R \subseteq A \times B$ binární relace mezi množinami A a B, pak <u>*inverzní relací*</u> k relaci R rozumíme relaci $R^{-1} \subseteq B \times A$ takovou, že $\forall\ a \in A,\ b \in B$; $(b, a) \in R^{-1} \Leftrightarrow (a, b) \in R$. <u>*Relací doplŘkovou*</u> k relaci R rozumíme relaci $R' = A \times B \setminus R$.

Definice 2.2.5 Nechť $R \subseteq A \times B$, $S \subseteq B \times C$. Pak <u>*sloǵením binárních relací R*</u> a S (v tomto pořadí) nazýváme binární relaci $\square \cdot \square \subseteq A \times C$ takovou, že $\forall\ a \in A,\ c \in C$; $(a, c) \in \square \cdot \square \Leftrightarrow$ $(\exists b \in B;\ (a, b) \in R \wedge (b, c) \in S)$.

Definice 2.2.6 <u>*Zobrazením f mnoǵiny A do mnoǵiny B*</u> rozumíme korespondenci mezi A a B takovou, že

1) Dom$f = A$ (neboli pro každé $x \in A$, $\exists y \in B$ tak, že $(x, y) \in f$),

2) Pro každé $x \in A$ a $y_1, y_2 \in B$ platí : jestliže $(x, y_1) \in f$, $(x, y_2) \in f$, pak $y_1 = y_2$.

Pro zobrazení f množiny A do množiny B užíváme rovněž označení $f : A \to B$. Místo $(x, y) \in f$ píšeme také $f(x) = y$. Je-li f zobrazení množiny A do množiny A (tj. $A = B$), hovoříme o zobrazení množiny A do sebe. *Transformací množiny A* rozumíme zobrazení A do A.

Definice 2.2.7 Nechť f je zobrazení množiny A do množiny B. Říkáme, že f je

a) *zobrazení prosté* (*injektivní, injekce*) A do B, má-li následující vlastnost :

Pro každé $x_1, x_2 \in A$ a $y \in B$ platí : jestliže $(x_1, y) \in f$, $(x_2, y) \in f$, pak $x_1 = x_2$.

b) *zobrazení A na B* (*surjektivní, surjekce*), má-li vlastnost :

$\mathrm{Im} f = B$ (neboli pro každé $y \in B$, $\exists x \in A$ tak, že $(x, y) \in f$),

c) *vzájemně jednoznačné zobrazení A na B* (*bijektivní, bijekce*), je-li současně injektivní i surjektivní.

Bijekce množiny na sebe se nazývá *permutace.*

Otázky

1. Co rozumíme pojmem kartézský součin množin?
2. Co rozumíme binární relací mezi množinami?
3. Co rozumíme pojmem binární relace na množině?
4. Kdy řekneme, že relace je na dané množině reflexivní?
5. Kdy řekneme, že relace je na dané množině symetrická?
6. Kdy řekneme, že relace je na dané množině antisymetrická?
7. Kdy řekneme, že relace je na dané množině tranzitivní?
8. Co rozumíme uspořádanou množinou?
9. Co rozumíme řetězcem?
10. Co je to relace ekvivalence?
11. Co rozumíme rozkladem množiny?
12. Co rozumíme zobrazením množiny do množiny?
13. Co rozumíme definičním oborem a oborem hodnot daného zobrazení?
14. Kdy řekneme, že dané zobrazení je prosté?
15. Kdy řekneme, že dané zobrazení je surjektivní?
16. Co je to bijekce?
17. Co je to permutace?

Cvičení

1) Je dána množina $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$
   a) Určete výčtem prvků binární relaci $R = \{(x, y) \in A^2;\ x \mid y \wedge 1 < x < y\}$,
   b) Určete definiční obor a obor hodnot relace R,
   c) Určete výčtem prvků relaci R^{-1} inverzní k R,
   d) Určete výčtem prvků relaci R' doplňkovou k R,
   e) Znázorněte relace R, R^{-1} a R' pomocí kartézského a uzlového grafu.

2) Na množině $M = \{1, 2, 3, 4, 5, 6\}$ jsou definovány binární relace R_1, R_2, R_3 a R_4 pomocí následujících výrokových forem: R_1: x je násobkem y, R_2: x není násobkem y, R_3: x je dělitelem y a R_4: x není dělitelem y.
   a) Určete výčtem prvků binární relace R_1, R_2, R_3 a R_4,
   b) Nakreslete kartézské a uzlové grafy těchto relací.

3) Je dána množina $A = \{a, b, c, d\}$ a relace $S\ \{(a, b), (b, a), (c, b)\} \subseteq A^2$. Určete vlastnosti relace S. Dále doplňte danou relaci o co nejméně uspořádaných dvojic z A^2 tak, aby vznikla relace, která bude na množině A:
   a) reflexivní,
   b) symetrická,
   c) reflexivní a symetrická,
   d) tranzitivní,
   e) ekvivalencí.

4) Uveďte příklad množiny A a relace R, která na množině A:
   a) je reflexivní,
   b) není reflexivní,
   c) je symetrická,
   d) není symetrická,
   e) je antisymetrická,
   f) není antisymetrická,
   g) je tranzitivní,
   h) není tranzitivní,
   i) je ekvivalencí,
   j) je uspořádáním, které není lineární,
   k) je lineárním uspořádáním,
   l) je symetrická a antisymetrická.

5) Určete vlastnosti relace R na vhodné množině M, jestliže výroková forma xRy znamená:
   a) x je služebně podřízen y,
   b) x je starší než y,
   c) x chodí do téže třídy jako y,
   d) x je manželkou y,
   e) x není mladší než y,
   f) x je potomkem y,
   g) x je předkem y.

6) Jsou dány množiny $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $C = \{♣, ♦, ♥, ♠\}$ a relace $R = \{(1, b), (1, c), (2, a), (3, a)\}$, $S = \{(a, ♥), (b, ♣), (b, ♥), (c, ♠)\}$ a $T = \{(♦, a), (♣, b), (♠, a)\}$. Určete složené relace □ · □, □ · □, □ · □, □ · □.

7) Určete vlastnosti následujících relací:
   a) $R_1 = \{(x, y) \in N^2;\ 2 \mid (x+y)\}$,
   b) $R_2 = \{(x, y) \in R^2;\ x = 2y\}$,
   c) $R_3 = \{(x, y) \in N^2;\ x+y \geq 5\}$,
   d) $R_4 = \{(x, y) \in R^2;\ x \neq y\}$,
   e) $R_5 = \{(x, y) \in \rho_p{}^2;\ x$ je rovnoběžná s $y\}$, kde ρ_p je množina všech přímek v rovině ρ,
   f) $R_6 = \{(x, y) \in Z^2;\ |x| \geq |y|\}$,

g) $R_7 = \{(x, y)\in Z^2;\ x^2 = y\}$,
h) $R_8 = \{(x, y)\in R^2;\ x^2 + y^2 = 1\}$,
i) $R_9 = \{(x, y)\in R^2;\ x - y = 2k\pi$, kde k je libovolné celé číslo$\}$,
j) $R_{10} = \{(x, y)\in A^2;\ x \mid y\}$, kde A je množina všech přirozených dělitelů čísla 12,
k) $R_{11} = \{(x, y)\in P(A)^2;\ x \subseteq y\}$, kde $A = \{1, 2, 3\}$.

8) Rozhodněte, které z relací z předchozího cvičení jsou relace ekvivalence, případně určete příslušný rozklad.

9) Rozhodněte, které z relací z cvičení 7) jsou relace uspořádání (resp. lineární uspořádání), případně je graficky znázorněte (Hasseův diagram).

10) Nakreslete Hasseův diagram uspořádané množiny, která
a) má největší prvek a nemá nejmenší prvek,
b) má dva různé maximální prvky,
c) má tři různé minimální prvky,
d) nemá maximální prvek,
e) nemá maximální prvek ani minimální prvek.

11) Rozhodněte, které z relací z cvičení 7) jsou zobrazení, případně určete vlastnosti tohoto zobrazení (injektivní, surjektivní, bijektivní).

12) Nechť X, Y jsou neprázdné množiny. Uvažujme množiny: R je množina všech binárních relací mezi X a Y, Z je množina všech zobrazení mezi X a Y, S je množina všech surjektivních zobrazení mezi X a Y, I je množina všech injektivních zobrazení mezi X a Y a B je množina všech bijektivních zobrazení mezi X a Y. Nakreslete Vennův diagram znázorňující vztah množin R, Z, S, I a B.

13) Určete výčtem prvků všechny binární relace na množině $M = \{a, b\}$. Dokážete předem určit jejich počet? Které z nich budou reflexivní?

14) Na základě předchozího cvičení určete počet všech binárních relací na tříprvkové množině. Kolik z nich bude reflexivních?

15) Udejte nutnou a postačující podmínku pro to, aby relace $\subseteq$ (množinová inkluze) byla symetrickou relací na potenční množině $P(A)$.

16) Určete všechny různé rozklady množiny $M = \{a, b, c\}$ a pro každý rozklad určete jemu příslušnou relaci ekvivalence.

17) Určete vlastnosti následujících zobrazení:
a) f_1: $C \to R$, $f_1(x + yi) = x$,
b) f_2: $C \to R^2$, $f_2(x + yi) = (x, y)$,
c) f_3: $R^2 \to R^3$, $f_3((x, y)) = (x + 1, y, x)$,
d) f_4: $R^3 \to R^3$, $f_4((x, y, z)) = (x - y, x - 2y, x - 3z)$,
e) f_5: $R^n \to R$, $f_5((x_1, \text{é}, x_n)) = x_1 + \text{é} + x_n$,
f) f_6: $R^n \to R^n$, $f_6((x_1, \text{é}, x_n)) = (x_1, x_1 + x_2, \text{é}, x_1 + x_2 + \ldots + x_n)$,
g) f_7: $N^2 \to N$, $f_7((x, y)) = x + y$,
h) f_8: $N \to N^2$, $f_8(x) = (2x, 2x + 1)$,

i) f_9: $N^2 \to P(N)$, $f_9((x, y)) = \{x, y\}$,

18) Uveďte příklad množin A a B a zobrazení f: $A \to B$, tak, aby f:
   a) bylo surjektivní,
   b) nebylo surjektivní,
   c) bylo injektivní,
   d) nebylo injektivní,
   e) bylo bijektivní.

19) Určete vlastnosti zobrazení (funkce jedné reálné proměnné) f: $R \to R$, $f(x) = ax + b$ v závislosti na koeficientech $a, b \in R$.

20) Zobrazení z předchozího cvičení je lineární funkce, kterou znáte ze střední školy. Projděte si ostatní základní elementární funkce jedné reálné proměnné (kvadratickou, mocninnou, exponenciální, logaritmickou, goniometrické funkce, …) a určete jejich vlastnosti.

3 Algebraické struktury

3.1 Algebraické struktury s jednou binární operací

Cíle

Po prostudování této kapitoly dokážete:

- porozumět obsahu pojmů binární operace na množině a algebraická struktura s jednou binární operací,
- správně používat příslušnou terminologii a symboliku,
- samostatně určovat základní vlastnosti operací a rozlišovat základní struktury s jednou binární operací.

Každé zobrazení f kartézského součinu M^n do množiny M nazýváme *n-ární operací na množině M*. Operace f tedy přiřazuje každé uspořádané n-tici $(m_1, m_2, ..., m_n) \in M^n$ právě jeden prvek $m \in M$, což zapisujeme $f(m_1, m_2, ..., m_n) = m$. Je-li $n = 2$, mluvíme o *binární operaci na množině M* a místo $f(m_1, m_2) = m$ píšeme častěji $m_1 f m_2 = m$. Symbol f pro označení binární operace pak zpravidla nahrazujeme některým ze symbolů $\bullet$, $*$, $+$, $\cdot$, $\times$ apod.

Definice 3.1.1 *Grupoidem* $G = (G, \cdot)$ nazveme neprázdnou množinu G s binární operací „·“ definovanou na této množině.

Je-li operace „·“ navíc komutativní, t.j. $\forall a, b \in G : a \cdot b = b \cdot a$, nazývá se G *komutativní grupoid*.

Definice 3.1.2 Řekneme, že grupoid $G = (G, \cdot)$ má *neutrální prvek* n, jestliže existuje $n \in G$ takový, že $\forall a \in G : a \cdot n = a = n \cdot a$.

Definice 3.1.3 Nechť grupoid $G = (G, \cdot)$ má neutrální prvek n a nechť $a \in G$. Pak prvek $a^{-1} \in G$ se nazývá *inverzním prvkem k prvku* a, platí-li $a \cdot a^{-1} = n = a^{-1} \cdot a$.

Definice 3.1.4 Pologrupou rozumíme libovolný grupoid $G = (G, \cdot)$, ve kterém je operace „· „ asociativní, t.j. $\forall a,b,c \in G : a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice 3.1.5 Pologrupa $G = (G, \cdot)$ se nazývá grupou, obsahuje-li neutrální prvek a existuje-li v ní ke každému prvku prvek inverzní.

Otázky

1. Co rozumíme binární operací na množině?
2. Co rozumíme grupoidem?
3. Co rozumíme pologrupou?
4. Co rozumíme grupou?
5. Co rozumíme komutativní grupou?
6. Je každá grupa pologrupou?
7. Je každá grupa grupoidem?
8. Je každá pologrupa grupoidem?
9. Je každá pologrupa grupou?
10. Je každý grupoid pologrupou?
11. Je každý grupoid grupou?

Cviļení

1) Uveďte konkrétní příklady binárních operací na množině.

2) Nakreslete Vennův diagram znázorňující třídu všech grupoidů, komutativních grupoidů, pologrup, komutativních pologrup, grup a komutativních grup.

3) Uveďte příklad nekomutativního grupoidu a znázorni jeho polohu v diagramu z cvičení 2).

4) Uveďte příklad grupoidu, který není pologrupou, a znázorni jeho polohu v diagramu z cvičení 2).

5) Uveďte příklad pologrupy, která není grupou, a znázorni její polohu v diagramu z cvičení 2).

6) Uveďte příklad nekomutativní grupy a znázorni její polohu v diagramu z cvičení 2).

7) Upravte Vennův diagram z cvičení 2) tak, aby rozlišil grupoidy s neutrálním prvkem a grupoidy bez neutrálního prvku. Zapiš do každého políčka tohoto diagramu aspoň jeden příklad grupoidu odpovídajících vlastností.

8) Je dána množina $M = \{a, b, c\}$. Rozhodněte, které z následujících binárních relací mezi množinami $M\times M$ a M jsou binárními operacemi na množině M, případně je zapište pomocí Cayleyovy tabulky:

$R_1 = \{((a, a), b),\ ((a, b), b),\ ((a, c), b),\ ((c, c), a)\}$,
$R_2 = \{((a, b), c),\ ((b, a), c),\ ((b, c), a),\ ((a, c), b)\ ((a, b), a)\}$,
$R_3 = \{((a, a), b),\ ((a, b), a),\ ((a, c), c),\ ((c, c), c)\ ((b, a), a),\ ((b, b), a),\ ((b, c), c),$
$((c, a), c),\ ((c, b), c),\ \}$.

9) Rozhodněte, zda se v následujících případech jedná o binární operace na příslušných množinách:
   a) sčítání na Z_0,
   b) sčítání na ⍰⍰,
   c) odčítání na N,
   d) odčítání na Z,
   e) sčítání na $\{-1, 1\}$,
   f) sčítání na $R\backslash Q$,
   g) násobení na C_0,
   h) násobení na ⍰⍰,
   i) násobení na $R\backslash Q$,
   j) násobení na $\{-1, 1\}$,
   k) dělení na Z,
   l) dělení na Q,
   m) dělení na Q_0,
   n) odčítání na C,
   o) umocňování na Z,
   p) umocňování na Q,
   q) umocňování na R,
   r) sčítání matic na $M_{mxn}(T)$,
   s) násobení matic na $M_{mxn}(T)$,
   t) násobení matic na $M_n(T)$,
   u) skládání transformací na množině všech transformací neprázdné množiny A,
   v) skládání permutací na množině všech permutací neprázdné množiny A,
   w) skalární součin vektorů na množině všech vektorů daného eukleidovského vektorového prostoru,
   x) vektorový součin vektorů na množině všech vektorů daného eukleidovského vektorového prostoru,

10) Rozhodněte, zda jsou obvyklé sčítání a násobení binárními operacemi na množině M, kde M je množina:
   a) všech sudých celých čísel,
   b) všech lichých celých čísel,
   c) všech celočíselných násobků pěti,
   d) všech záporných racionálních čísel,
   e) všech kladných racionálních čísel,
   f) všech iracionálních čísel,
   g) všech imaginárních čísel,
   h) všech ryze imaginárních čísel,

i) všech komplexních jednotek,
j) všech komplexních druhých odmocnin z jedné,
k) všech komplexních třetích odmocnin z jedné,
l) všech komplexních čtvrtých odmocnin z jedné.

11) Nechť na množině $A = \{0, 1, 2\}$ je definována binární operace $*$ takto: $\forall x, y \in A$; $x * y$ se rovná zbytku při dělení čísla $x^2 - y^2$ číslem 3. Sestavte Cayleyovu tabulku operace „$*$“ a zjistěte, je-li tato operace komutativní a asociativní.

12) Na množině všech racionálních čísel Q definujme operaci $*$ takto: $x * y = \frac{\square\square\square}{\square}$. Vyšetřete vlastnosti grupoidu $(Q, *)$.

13) Nechť $A = \{(a, b);\ a, b \in R,\ a \neq 0\}$. Definujme binární operaci $*$ na A takto: $(a, b) * (c, d) = (ac, bc + d)$. Určete vlastnosti grupoidu $(A, *)$.

14) Nechť pro libovolná reálná čísla a, b platí: $a \bullet b = a + b + 2$, $a * b = a + b + ab$. Dokažte, že $(R, \bullet)$ je komutativní grupa a $(R, *)$ je komutativní pologrupa s neutrálním prvkem, která není grupou.

15) Označme M množinu všech matic ve tvaru

a) $\begin{pmatrix} \square & \square \\ 0 & \square \end{pmatrix}$ b) $\begin{pmatrix} \square & 0 \\ \square & 1 \end{pmatrix}$,

kde $x, y \in R$, $x \neq 0$. Ověřte, zda množina M tvoří spolu s operací násobení matic grupoid a určete vlastnosti tohoto grupoidu.

16) Rozhodněte, kolika způsoby lze doplnit následující tabulku operace $*$ na množině $G = \{a, b, c\}$ tvaru

$*$	a	b	c
a	c	b	a
b	.	.	b
c	.	.	.

tak, aby $(G, *)$

a) byl grupoid,
b) byl grupoid s jedničkou,
c) byl komutativní grupoid,
d) byla komutativní pologrupa,
e) byla pologrupa s jedničkou,
f) byla grupa.

17) Sestavte Cayleyovu tabulku pro sčítání „$\oplus$“ a násobení „$\otimes$“ na množině Z_3 zbytkových tříd modulo 3 a určete vlastnosti grupoidů $(Z_3, \oplus)$ a $(Z_3, \otimes)$.

18) Sestavte Cayleyovu tabulku pro sčítání „$\oplus$“ a násobení „$\otimes$“ na množině Z_4 zbytkových tříd modulo 4 a určete vlastnosti grupoidů $(Z_4, \oplus)$ a $(Z_4, \otimes)$.

19) Určete množinu $S(A)$ všech permutací na množině $A = \{1, 2, 3\}$ a sestavte Cayleyovu tabulku pro skládání permutací z $S(A)$. Ukažte, že množina $S(A)$ tvoří spolu s operací skládání permutací grupu, která není komutativní.

20) Nechť ρ je rovina. Označme pro libovolné body $A, B \in \rho$ symbolem $A*B$ střed úsečky AB. Určete vlastnosti grupoidu $(\rho, *)$.

21) Určete podmínku, kterou musí splňovat množina M, aby grupoid $(P(M), \cap)$ měl vlastnosti grupy ($P(M)$ značí tzv. potenční množinu množiny M, tj. množinu všech podmnožin v M).

22) Určete podmínku, kterou musí splňovat množina M, aby grupoid $(P(M), \cup)$ měl vlastnosti grupy.

3.2 Algebraické struktury se dvěma binárními operacemi

Cíle

Po prostudování této kapitoly dokážete:

- porozumět obsahu pojmů binární operace na množině a algebraická struktura se dvěma binárními operacemi,
- správně používat příslušnou terminologii a symboliku,
- samostatně určovat základní vlastnosti operací a rozlišovat základní struktury se dvěma binárními operacemi.

Definice 3.2.1 *Polookruhem* nazýváme algebraickou strukturu $M = (M, +, \cdot)$ se dvěma binárními operacemi „+“ a „$\cdot$ „ takovou, že $(M,+)$ je komutativní pologrupa, $(M, \cdot)$ je pologrupa a operace „$\cdot$ „ je distributivní vzhledem k operaci „+“, t.j. $\forall a, b, c \in M$ platí :

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

Je-li $(M, \cdot)$ navíc komutativní, říkáme, že $(M, +, \cdot)$ je *komutativní polookruh*.

Obsahuje-li algebraická struktura $(M, +, \cdot)$ neutrální prvky vzhledem k oběma operacím, nazýváme z důvodu rozlišení neutrální prvek vzhledem k operaci „+“ *nulovým prvkem* (nebo stručně *nulou*) a neutrální prvek vzhledem k operaci „$\cdot$“ *jednotkovým prvkem* (stručně *jedničkou*). Nulový prvek budeme značit symbolem o a jednotkový symbolem e. V některých případech, kdy nebude hrozit nedorozumění, budeme nulový prvek rovněž značit symbolem 0 a jednotkový prvek symbolem 1.

Definice 3.2.2 Polookruh $(M, +, \cdot)$ obsahující jednotkový prvek se nazývá *polookruh s jednotkovým prvkem* nebo krátce *polookruh s jedničkou*.

Definice 3.2.3 Polookruh $M = (M, +, \cdot)$ nazveme *okruhem*, je-li $(M, +)$ komutativní grupou.

Definice 3.2.4 Prvek $a \neq o$ okruhu $(M,+, \cdot)$ se nazývá *netriviálním dělitelem nuly*, existuje-li nenulový prvek $b \in M$ takový, že $a \cdot b = o$, $b \cdot a = o$.

Definice 3.2.5 *Oborem integrity* budeme rozumět každý komutativní okruh $J = (J, +, \cdot)$ s jedničkou $e \neq o$, v němž neexistují netriviální dělitelé nuly.

Definice 3.2.6 Každý alespoň dvouprvkový okruh $T = (T, +, \cdot)$ takový, že $(T \setminus \{o\}, \cdot)$ je grupa, se nazývá *těleso*.

Definice 3.2.7 a) Řekneme, že těleso T má *charakteristiku* k ($k \in N$), jestliže k je nejmenší přirozené číslo takové, že $k \times e = o$. (symbol „×“ značí tzv. *přirozený násobek*, tj. $k \times e = e + e + \dots + e$ - k sčítanců).

b) Jestliže takové přirozené číslo k neexistuje, pak říkáme, že těleso T je *nekonečné chrakteristiky* (nebo, že má *charakteristiku* 0).

Uvedené definice základních algebraických pojmů by měly umožnit i čtenáři, který není obeznámen s problematikou binárních relací, zobrazení a algebraických struktur, zorientovat se v následujícím textu. Další podrobnější popis vlastností definovaných struktur lze nalézt v příslušné literatuře, proto zde od něj upouštíme, abychom zbytečně nezvětšovali rozsah skripta.

Otázky

1. Co rozumíme algebraickou strukturou se dvěma binárními operacemi?
2. Co rozumíme polookruhem?
3. Co je to okruh?
4. Jaké vlastnosti má obor integrity?
5. Co rozumíme tělesem?
6. Je každý okruh polookruhem?
7. Je každý polookruh okruhem?
8. Je každý okruh polookruhem?
9. Je každý okruh oborem integrity?
10. Je každý obor integrity okruhem?
11. Je každý obor integrity tělesem?
12. Je každé těleso oborem integrity?
13. Je každé těleso okruhem?
14. Co rozumíme charakteristikou tělesa?

Cvičení

1) Nakreslete Vennův diagram znázorňující třídu všech okruhů, komutativních okruhů, okruhů s jedničkou, oborů integrity, těles a komutativních těles.

2) Uveďte příklad nekomutativního okruhu a znázorni jeho polohu v diagramu z cvičení 1).

3) Uveďte příklad okruhu bez jedničky a znázorni jeho polohu v diagramu z cvičení 1).

4) Uveďte příklad komutativního okruhu s jedničkou, která není oborem integrity, a znázorni její polohu v diagramu z cvičení 1).

5) Uveďte příklad oboru integrity, který není tělesem, a znázorni jeho polohu v diagramu z cvičení 1).

6) Uveďte příklad tělesa, které není oborem integrity, a znázorni jeho polohu v diagramu z cvičení 1).

7) Rozhodněte, zda se v následujících případech jedná o okruhy, případně určete jejich další vlastnosti (komutativnost, existence jednotkového prvku, existence dělitelů nuly, je-li daný okruh oborem integrity, příp. tělesem):
   a) $(2Z+1, +, \cdot)$,
   b) $(2Z, +, \cdot)$,
   c) $(3Z+1, +, \cdot)$,
   d) $(3Z, +, \cdot)$,
   e) $(Q_0, +, \cdot)$,
   f) $(R\setminus Q, +, \cdot)$,
   g) $(\{-1, 1\}, +, \cdot)$,
   h) $(R, \bullet, *)$, kde $\forall a, b \in R$ platí: $a \bullet b = a + b + 2$, $a * b = a + b + ab$,
   i) $(M, +, \cdot)$, kde $M = \{\begin{pmatrix} [illegible] & [illegible] \\ 2[illegible] & [illegible] \end{pmatrix}; a, b \in R\}$, „+“ a „·“ je sčítání a násobení matic,
   j) $(Z_3, \oplus, \otimes)$, kde Z_3 jsou zbytkové třídy modulo 3, „⊕“ a „⊗“ je sčítání a násobení zbytkových tříd,
   k) $(Z_4, \oplus, \otimes)$, kde Z_4 jsou zbytkové třídy modulo 4, „⊕“ a „⊗“ je sčítání a násobení zbytkových tříd,
   l) $(Z[\sqrt{2}], +, \cdot)$, kde $Z[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in Z\}$,
   m) $(Q(\sqrt{3}), +, \cdot)$, kde $Q(\sqrt{3}) = \{a + b\sqrt{3}; a, b \in Q\}$.

4 Logická struktura matematického textu a výkladu

4.1 Definice matematických pojmů

Cíle

Po prostudování této kapitoly dokážete:

- porozumět tomu, co je obsah a rozsah matematického pojmu,
- správně pochopit, co rozumíme definicí matematického pojmu,
- samostatně určovat základní části definice – definiendum, definiens,

- rozhodnout o správnosti formulace definice daného pojmu,
- rozhodnout o vztahu rozsahů definovaných pojmů.

Každý matematický pojem má určitý *obsah* a *rozsah*. *Obsah* pojmu tvoří souhrn všech vlastností, které jsou pro daný pojem charakteristické. Např. obsahem pojmu rovnoběžník je „rovinný obrazec ohraničený čtyřmi úsečkami, jehož protilehlé strany a úhly jsou shodné, úhlopříčky se vzájemně půlí, atd.“. *Rozsah* pojmu tvoří množina všech objektů, které mají všechny vlastnosti stanovené jeho obsahem. Rozsahem pojmu rovnoběžník je tedy množina všech rovnoběžníků. Rozšiřujeme-li obsah pojmu, zúží se jeho rozsah a obráceně. Je-li rozsah jednoho pojmu obsažen v rozsahu druhého pojmu, říkáme, že druhý pojem je *rodem* (*rodovým pojmem*) vzhledem k prvnímu pojmu a naopak první pojem je *druhem* (*druhovým pojmem*) druhého pojmu. Např. pojem obdélník je rodovým pojmem pojmu čtverec a pojem čtverec je druhovým pojmem pojmu obdélník. Můžeme tedy říci, že každý čtverec je obdélníkem, ale ne naopak.

Definicí rozumíme část textu nebo výkladu, která slouží k zavedení nového pojmu. Z formálního hlediska definice zpravidla obsahuje tzv. *definiendum*, tj. výraz, který je definován (jehož obsah definicí vymezujeme) a *definiens*, tj. výraz, pomocí něhož je vymezen obsah definienda. Obě tyto části definice jsou spojeny *definiční rovností* (např. slovním obratem „znamená“, „je“, „rozumíme“, „nazýváme“, „je definován jako“, apod.), případně *definiční ekvivalencí* („právě když“, „tehdy a jen tehdy“, …ale také „jestliže, pak“).

Příklady

a) Čtvercem rozumíme rovnostranný pravoúhlý čtyřúhelník.
b) Prvočíslem nazveme přirozené číslo, které má právě dva různé dělitele.
c) Jestliže pro přirozená čísla a, b platí $a = bx$, kde x je přirozené číslo, říkáme, že číslo a je násobkem čísla b (číslo b je dělitelem čísla a).

Při nesprávné formulaci definice může dojít k porušení definiční rovnosti (definiční ekvivalence) třemi způsoby:

1) *zužující definice* – rozsah definiens je menší, než rozsah definienda (např. „Funkce $y = ax^2+bx$, kde $a \neq 0$, se nazývá kvadratická),
2) *rozšiřující definice* - rozsah definiens je větší, než rozsah definienda (např. „Čtverec je pravidelný čtyřúhelník“),
3) *posunující definice* – některé objekty jsou do rozsahu pojmu nesprávně zahrnuty a naopak, jiné objekty jsou nesprávně nezařazeny (např. „ Funkce $y = ax^2+bx$ se nazývá kvadratická).

Nepřípustnou logickou chybou při formulaci definice je definování neznámého pojmu pomocí jiného neznámého pojmu, příp. tzv. *definice kruhem*, kdy v definiens se objevuje stejný pojem jako v definiendu (např. „Báze vektorového prostoru je taková báze …“).

Otázky

1. Co rozumíme obsahem a rozsahem matematického pojmu?
2. Co rozumíme definicí matematického pojmu?
3. Co je definiendum a definiens?
4. Co rozumíme definiční rovností?
5. Co rozumíme definiční ekvivalencí?

6. Co rozumíme zužující definicí?
7. Co rozumíme rozšiřující definicí?
8. Co rozumíme posunující definicí?
9. Co je to definice kruhem?

Cviļ ení

1) Pokuste se definovat následující pojmy:
   a) obdélník,
   b) kosočtverec,
   c) kosodélník,
   d) kružnice,
   e) kruh,
   f) kvadratická funkce,
   g) lineární funkce,
   h) rovnost zlomků,
   i) podobnost trojúhelníků,
   j) binární relace na množině,
   k) zobrazení mezi množinami,
   l) binární operace na množině,
   m) grupa,
   n) komutativní těleso,
   o) vektorový prostor,
   p) lineární kombinace vektorů,
   q) lineární obal podmnožiny vektorového prostoru,
   r) báze vektorového prostoru,
   s) dimenze vektorového prostoru,
   t) determinant čtvercové matice,
   u) hodnost matice,
   v) souřadnice vektoru vzhledem k dané bázi,
   w) eukleidovský vektorový prostor.

2) Rozhodněte o správnosti formulace následujících definic, případně uveďte, o který typ porušení definiční symetrie se jedná a zformulujte správnou definici:
   a) Funkce $y = ax^2+bx+c$ se nazývá kvadratická,
   b) Funkce $y = x^2+bx+c$ se nazývá kvadratická,
   c) Jestliže pro přirozená čísla a, b platí $a = bx$, kde x je racionální číslo, říkáme, že číslo a je násobkem čísla b (číslo b je dělitelem čísla a).
   d) Iracionální jsou čísla, která nejsou racionální.
   e) Ryze imaginárním číslem rozumíme každé číslo tvaru bi, kde b je reálné číslo.
   f) Binární relací na množině A rozumíme každou neprázdnou podmnožinu kartézského součinu A^2.
   g) Zobrazením množiny A do množiny B rozumíme binární relaci, která každému prvku z A přiřadí nejvýše jeden prvek z B.
   h) Algebraickou strukturu s jednou binární operací, v níž existuje neutrální prvek a ke každému prvku prvek symetrický, nazveme grupou.
   i) Tělesem rozumíme obor integrity, v němž všechny nenulové prvky tvoří grupu vzhledem k násobení.
   j) Matici nazveme diagonální, jestliže všechny její prvky, které neleží na hlavní diagonále jsou rovny nule.

k) Jsou-li A a B neprázdné množiny, pak levou vnější operací nad A a B rozumíme každé zobrazení $\bullet : A\times B \to A$.
l) Řekneme, že vektory [illegible], …, [illegible] $\in R^n$ jsou lineárně závislé, jestliže existují reálná čísla $c_1, \dots, c_k$ taková, že c_1 [illegible] $+ \dots +$ c_k [illegible] $=$ [illegible]
m) Lineárním obalem podmnožiny M vektorového prostoru V rozumíme průnik všech podprostorů prostoru V obsažených v množině M.
n) Bází vektorového prostoru konečné dimenze rozumíme jeho libovolnou množinu generátorů.
o) Hodností matice rozumíme počet jejích lineárně nezávislých řádků.

3) Definujte pojmy čtverec, pravoúhelník, rovnoběžník, čtyřúhelník, mnohoúhelník a rovinný obrazec a rozhodněte, v jakém vztahu jsou rozsahy těchto pojmů.

4.2 Matematické věty

Cíle

Po prostudování této kapitoly dokážete:

- porozumět významu matematických vět v matematickém výkladu,
- správně se orientovat v obvyklých formulacích matematických vět,
- správně používat příslušnou terminologii a symboliku,
- využívat základních poznatků matematické logiky při modifikování matematických vět,

Matematickou větou (*poučkou*) rozumíme zpravidla určitý matematický poznatek vyjádřený slovy nebo symbolickým zápisem, přičemž předpokládáme jeho platnost (zaručenou důkazem). Z hlediska logiky je tedy matematická věta pravdivým výrokem o vlastnostech matematických pojmů. Matematické věty mívají většinou tvar implikace $A \Rightarrow B$, nebo je lze na tento tvar převést. Výrok A nazýváme *předpokladem* (*postačující podmínkou*, *antecedentem*) a výrok B *tvrzením* (*nutnou podmínkou*, *konsekventem*).
K matematické větě tvaru $A \Rightarrow B$ můžeme vytvořit *větu obrácenou* $B \Rightarrow A$ a *větu obměněnou* $\neg B \Rightarrow \neg A$. Zatímco věta obrácená platit nemusí (tj. nemusí být matematickou větou), věta obměněná má vždy stejnou pravdivostní hodnotu jako věta původní (přesvědčte se pomocí tabulky pravdivostních hodnot!). Platí-li pro danou matematickou větu tvaru $A \Rightarrow B$ i věta obrácená $B \Rightarrow A$, můžeme obě věty formulovat jako větu jedinou ve tvaru ekvivalence $A \Leftrightarrow B$ (příp. $B \Leftrightarrow A$)

Otázky

1. Co rozumíme matematickou větou?
2. Jaký je obvyklý tvar matematické věty?
3. Co rozumíme předpokladem a tvrzením matematické věty?
4. Kdy říkáme, že matematická věta udává nutnou a postačující podmínku?
5. Co rozumíme větou obrácenou k dané větě a co můžeme říci o její pravdivosti?
6. Co rozumíme větou obměněnou k dané větě a co můžeme říci o její pravdivosti?

Cvičení

1) Určete předpoklad a tvrzení následujících matematických vět:
   a) Úhlopříčky v rovnoběžníku se půlí.
   b) Součet vnitřních úhlů v trojúhelníku je 180^0.

2) K následujícím matematickým větám utvořte větu obrácenou a obměněnou a rozhodněte o pravdivosti věty obrácené:
   a) Jsou-li obrazce shodné, mají stejný obsah.
   b) Je-li $x = 2$, pak $x^2 = 4$.
   c) Je-li x racionální číslo, je také x^2 racionální číslo.
   d) Je-li ciferný součet daného čísla dělitelný třemi, pak je toto číslo dělitelné třemi.
   e) Je-li číslo dělitelné dvěma a třemi, je dělitelné šesti.
   f) Je-li $(G, \cdot)$ grupa, je $(G, \cdot)$ pologrupa.
   g) Je-li $(G, +, \cdot)$ komutativní těleso, je $(G, +, \cdot)$ obor integrity .
   h) Má-li funkce f v bodě x_0 derivaci, je funkce f v bodě x_0 spojitá.
   i) Jestliže funkce f má v bodě a nenulovou derivaci, pak v tomto bodě nemá lokální extrém.

3) Zformulujte Pythagorovu větu, utvořte větu k ní obrácenou a obměněnou a rozhodněte o jejich pravdivostech.

4) Určete podmínku, která
   a) je postačující, ale není nutná,
   b) je nutná, ale není postačující,
   c) je nutná a postačující,
   d) není nutná ani postačující

   pro to, aby kvadratická rovnice $ax^2 + bx + c = 0$ měla dvě různá reálná řešení.

5) Určete podmínku, která
   a) je postačující, ale není nutná,
   b) je nutná, ale není postačující,
   c) je nutná a postačující,
   d) není nutná ani postačující

   pro to, aby přirozené číslo x bylo dělitelné číslem 66.

6) Nechť A a B jsou konečné neprázdné množiny. Určete nutnou a postačující podmínku pro existenci
   a) injektivního zobrazení $f: A \to B$,
   b) surjektivního zobrazení $f: A \to B$,
   c) bijektivního zobrazení $f: A \to B$.

4.3 Důkazy matematických vět

Cíle

Po prostudování této kapitoly dokážete:

- porozumět významu důkazů matematických vět,

- orientovat se v základních typech důkazů,
- využívat základních poznatků matematické logiky při dokazování matematických vět,

4.3.1 DŢkaz pŚímý

Přímý důkaz je založen na tautologii
$((A \Rightarrow B_1) \wedge (B_1 \Rightarrow B_2) \wedge \ldots \wedge (B_n \Rightarrow B)) \Rightarrow (A \Rightarrow B)$ (tranzitivnost implikace). Máme-li tedy dokázat větu ve tvaru implikace $A \Rightarrow B$, dokážeme postupně řetězec implikací $(A \Rightarrow B_1) \wedge (B_1 \Rightarrow B_2) \wedge \ldots \wedge (B_n \Rightarrow B)$, který začíná předpokladem dokazované věty (výrok A) a končí jejím tvrzením (výrok B). Díky uvedené tautologii odtud plyne platnost implikace $A \Rightarrow B$, tedy platnost dokazované věty.

PŚíklad
Dokažte, že pro každé přirozené číslo n platí: je-li n sudé, je n^2 sudé.
Přímým důkazem dokážeme větu $A \Rightarrow B$, kde A je výrok „n je přirozené sudé číslo“ a B je výrok „n^2 je sudé číslo“ :
Je-li n sudé, pak existuje $k \in N$ takové, že $n = 2k$ …………….. $A \Rightarrow B_1$
Je-li $n = 2k$, pak $n^2 = 4k^2$ …………………………………….. $B_1 \Rightarrow B_2$
Je-li $n^2 = 4k^2$, pak $n^2 = 2 \cdot 2n^2$ ……………………………….... $B_2 \Rightarrow B_3$
Je-li $n^2 = 2 \cdot 2n^2$, pak je n^2 sudé číslo ………………………… $B_3 \Rightarrow B$

4.3.2 DŢkaz nepŚímý

Nepřímým důkazem věty $A \Rightarrow B$ rozumíme přímý důkaz věty k ní obměněné, tj. věty $\neg B \Rightarrow \neg A$, která má vždy stejnou pravdivostní hodnotu jako věta $A \Rightarrow B$ (Využíváme tautologii $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$).

PŚíklad
Dokažte, že pro každé přirozené číslo n platí: je-li n^2 sudé, je n sudé.
Nepřímý důkaz věty $A \Rightarrow B$ je založen na přímém důkazu věty obměněné $\neg B \Rightarrow \neg A$, tj. věty „Je-li n liché, je n^2 liché.“
Je-li n liché, pak existuje $k \in N$ takové, že $n = 2k + 1$……………… ***é*** ……. $\neg B \Rightarrow B_1$
Je-li $n = 2k + 1$, pak $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1$ ……….. $B_1 \Rightarrow B_2$
Je-li $n^2 = 2 \cdot (2k^2 + 2k) + 1$, pak n^2 je liché číslo ……………………………. $B_2 \Rightarrow \neg A$

4.3.3 DŢkaz sporem

Předpokládáme, že věta $A \Rightarrow B$ neplatí, tedy platí její negace $\neg(A \Rightarrow B)$, kterou lze zapsat ve tvaru $A \wedge \neg B$. Od tohoto předpokladu dojdeme řetězcem implikací k evidentně nepravdivému výroku (sporu). To znamená, že předpoklad $\neg(A \Rightarrow B)$ neplatí a platí věta $A \Rightarrow B$.

PŚíklad
Dokažte, že $\sqrt{2}$ je iracionální číslo.

Předpokládáme platnost negace věty, tj., že $\sqrt{2}$ je číslo racionální a snažíme se vytvořit řetězec implikací, na jehož konci bude spor s tímto předpokladem.

Je-li $\sqrt{2}$ racionální číslo, pak existují nesoudělná čísla p, $q \in N$ taková, že $\sqrt{2} = \dfrac{p}{q}$

Jestliže $\sqrt{2} = \dfrac{p}{q}$, pak $2 = \dfrac{p^2}{q^2}$,

Je-li $2 = \dfrac{p^2}{q^2}$, pak $p^2 = 2q^2$, tj. p^2 je sudé číslo,
Je-li p^2 je sudé číslo, je p sudé číslo (viz předchozí příklad),
Je-li p sudé číslo, pak existuje $k \in N$ takové, že $p = 2k$,
Jestliže $p = 2k$, pak $2q^2 = p^2 = 4k^2$,
Jestliže $2q^2 = 4k^2$, pak $q^2 = 2k^2$, tj. q^2 je sudé číslo,
Je-li q^2 je sudé číslo, pak q je sudé číslo.
Dokázali jsme tedy, že p a q jsou sudá čísla, což je spor s předpokladem, že p a q jsou nesoudělná. To znamená, že náš předpoklad, že $\sqrt{2}$ je číslo racionální neplatí a platí jeho negace, tj. $\sqrt{2}$ je číslo iracionální.

PŚklad
Dokažte, že prvočísel je nekonečně mnoho.

Předpokládáme naopak, že $p_1, \ldots, p_n$ jsou všechna prvočísla. Uvažujme číslo $k = p_1 \cdot \ldots \cdot p_n + 1$. Kdyby číslo k bylo prvočíslem, muselo by se rovnat některému z čísel p_i. Ovšem číslo k dává po vydělení číslem p_i zbytek 1, což je spor. Pokud by číslo k bylo složené, muselo by být dělitelné některým z prvočísel p_i, což opět vede ke sporu.

4.3.4 DŢkaz matematickou indukcí

Důkaz matematickou indukcí představuje zvláštní případ přímého důkazu. Využívá následující specifické vlastnosti množiny všech přirozených čísel: Nechť $V(x)$ je výroková forma s oborem proměnnosti N. Je-li pravdivý výrok $V(n_0)$ pro některé $n_0 \in N$ a platí-li implikace $V(k) \Rightarrow V(k+1)$ pro každé $k \in N$, $k \geq n_0$, pak $V(n)$ je pravdivý výrok pro každé $n \in N$, $n \geq n_0$.

PŚklad
Dokažte, že pro každé $n \in N$ platí: $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Dokazovaná rovnost je vlastně výroková forma $V(n)$ o jedné proměnné n. Důkaz provedeme ve dvou krocích:

1) Ukážeme platnost $V(1)$:
   Pro $n = 1$ dostaneme $1 = 1^2$, tj. $V(1)$ platí.

2) Dokážeme platnost implikace $V(k) \Rightarrow V(k+1)$ pro každé $k \in N$:
   Předpokládáme tedy platnost rovnosti $V(k)$, tj.
   $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ (indukční předpoklad) a dokážeme, že z tohoto předpokladu plyne platnost $V(k+1)$, tj. rovnost
   $1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$.
   Budeme tedy upravovat levou stranu rovnosti $V(k+1)$ a s využitím indukčního předpokladu chceme dostat pravou stranu $V(k+1)$. Postupně dostaneme:

$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2$.

Kroky 1) a 2) dokazují platnost rovnosti $V(n)$ pro každé $n \in N$.

4.3.5 DŢkaz rovnosti dvou mnoĝin

PŚíklad

Dokažte, že pro libovolné množiny A, B, C platí $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

a) Pomocí Vennových diagramů – proveďte jako cvičení.
b) Pomocí tabulkové metody (viz např. [2]).
c) Pomocí „Principu neurčitého prvku“:

Abychom dokázali rovnost $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, dokážeme dvě inkluze: $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ a $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Nechť $x \in A \cap (B \cup C)$. Pak $x \in A$ a současně $x \in B \cup C$, tj. $x \in B$ nebo $x \in C$. Je-li $x \in B$, pak je $x \in A \cap B$, a je-li $x \in C$, je zřejmě $x \in A \cap C$. Tedy $x \in A \cap B$ nebo $x \in A \cap C$, tj. $x \in (A \cap B) \cup (A \cap C)$. Dokázali jsme tedy, že patří-li libovolný prvek do množiny $A \cap (B \cup C)$, patří rovněž do množiny $(A \cap B) \cup (A \cap C)$, neboli $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Podobným způsobem dokážeme i druhou inkluzi (dokažte jako cvičení).

Otázky

1. Jaké znáte základní typy důkazů matematických vět?
2. Na čem je založen přímý důkaz?
3. Na čem je založen nepřímý důkaz?
4. Na čem je založen důkaz sporem?
5. Jak provádíme důkaz matematickou indukcí?
6. Jak dokazujeme rovnost dvou množin?

Cviļení

1) Dokažte pomocí přímého důkazu věty:
   a) Tvoří-li kladná čísla $a_1, a_2, \ldots, a_n$ prvních n členů geometrické posloupnosti, potom $(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^2 = (a_1 \cdot a_n)^n$,
   b) $\forall x, y \in R; x^2 + y^2 \leq 2 \Rightarrow |x+y| \leq 2$,
   c) Je-li $tg 10^0$ racionální číslo, pak $cos 20^0$ je rovněž racionální číslo (využijte vzorec $cos 2x = \frac{[illegible]}{[illegible]}$).
   d) Jediným idempotentním prvkem každé grupy je její neutrální prvek.
   e) Jestliže v grupě $(G, \cdot)$ s neutrálním prvkem e platí $a \cdot a = e$ pro každé $a \in G$, pak je grupa $(G, \cdot)$ komutativní.

2) Dokažte pomocí nepřímého důkazu věty:
   a) Pro každé přirozené číslo n platí: Jestliže 3 dělí $n^2 + 2$, pak 3 nedělí n.
   b) Jestliže nelze sestrojit kružítkem a pravítkem úhel o velikosti 1^0, pak nelze takto sestrojit ani úhel o velikosti 19^0.
   c) Je-li $cos 20^0$ iracionální číslo, pak je $tg 10^0$ rovněž iracionální číslo.

3) Dokažte pomocí důkazu sporem věty:

a) Číslo $\sqrt{7}$ je iracionální.
b) Číslo $log7$ je iracionální.
c) Každým bodem A, který neleží na přímce p, prochází nejvýše jedna přímka q kolmá na přímku p.
d) V grupoidu existuje nejvýše jeden neutrální prvek.
e) V grupoidu existuje nejvýše jeden agresivní prvek.
f) V pologrupě s neutrálním prvkem existuje ke každému prvku nejvýše jeden symetrický prvek.
g) Žádné těleso neobsahuje netriviální dělitele nuly.
h) Nechť V je vektorový prostor, $u_1, \dots, u_n \in V$. Jestliže vektory $u_1, \dots, u_n$ jsou lineárně nezávislé pak neexistuje v množině $\{u_1, \dots, u_n\}$ podmnožina lineárně závislých vektorů.
i) Každá posloupnost reálných čísel má nejvýše jednu limitu.

4) Dokažte matematickou indukcí:
a) $\forall n \in N;\ 1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$,
b) $\forall n \in N;\ 1 + 2 + 3 + \dots + n = \frac{1}{2} n(n + 1)$,
c) $\forall n \in N;\ 1 + 3 + 5 + \dots + (2n - 1) = n^2$,
d) $\forall n \in N;\ 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{6} n(n + 1)(2n + 1)$,
e) $\forall n \in N;\ 1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4} n^2(n + 1)^2$,
f) $\forall n \in N;\ 2^{n-1} \leq n!$,
g) $\forall n \in N,\ n \geq 3;\ 2^n > 2n + 1$,
h) $\forall n \in N,\ n \geq 4;\ 3^n > n^3$,
i) $\forall n \in N,\ n \geq 5;\ 2^n > n^2$,
j) $\forall n \in N$; číslo $n^3 + 5n$ je dělitelné šesti.
k) $\forall n \in N$; číslo $2^{3n} + 3^{4n}$ není dělitelné číslem 73.
l) Je-li $n \in N$, $n \geq 2$, pak n různých přímek ležících v jedné rovině a procházejících jedním bodem dělí rovinu na $2n$ dutých úhlů.
m) Vzorec pro součet prvních n členů aritmetické posloupnosti.
n) Vzorec pro součet prvních n členů geometrické posloupnosti.
o) Binomickou větu.
p) Moivreovu větu.

5) Dokažte, že pro libovolné množiny A, B, C platí:
a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
b) $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$,
c) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$,
d) $(A \cap B)' = A' \cup B'$,
e) $(A \cup B)' = A' \cap B'$,
f) $C \times (A \cap B) = (C \times A) \cap (C \times B)$,
g) $C \times (A \cup B) = (C \times A) \cup (C \times B)$,
h) $C \times (A \setminus B) = (C \times A) \setminus (C \times B)$,

6) Dokažte nebo uveďte protipříklad:
a) Skládání binárních relací na dané množině je komutativní operace.
b) Skládání binárních relací na dané množině je asociativní operace.

c) Inverzní relace k relaci, která je zobrazením, je opět zobrazení.
d) Nechť A je neprázdná konečná množina a $f\colon A \to A$ zobrazení. Pak je-li f injekce nebo surjekce, pak f je již nutně bijekce.
e) Každá grupa je komutativní.
f) Existuje grupoid, který není pologrupou.
g) Žádný komutativní okruh s jedničkou neobsahuje netriviální dělitele nuly.
h) $(M_n(T), +)$ je komutativní grupa.
i) $(M_n(T), \cdot)$ je komutativní pologrupa.
j) $(M_n(T), +, \cdot)$ je okruh, který obsahuje netriviální dělitele nuly.
k) Nechť V je vektorový prostor, □ , …, □ $\in V$. Pak vektory □ , …, □ jsou lineárně nezávislé právě tehdy, když { □ , …, □} je bází prostoru V.
l) Nechť V je vektorový prostor, $M \subseteq V$, kde M ={ □ , …, □}. Pak existuje podmnožina $B \subseteq M$, která je bází prostoru V.
m) Vektory □ , …, □ z vektorového prostoru V jsou lineárně závislé právě tehdy, když aspoň jeden z nich je lineární kombinací ostatních.
n) Průnik dvou podprostorů vektorového prostoru V je opět podprostor prostoru V.
o) Sjednocení dvou podprostorů vektorového prostoru V je opět podprostor prostoru V.
p) Součet dvou podprostorů vektorového prostoru V je opět podprostor prostoru V.
q) Nechť $V \neq$ {□} je vektorový prostor konečné dimenze. Pak každé dvě jeho báze mají stejný počet prvků.
r) Hodnost matice je rovna počtu jejích lineárně nezávislých řádků.
s) Každá soustava lineárních rovnic je řešitelná.
t) Každá homogenní soustava lineárních rovnic je řešitelná.
u) Ke každé čtvercové matici existuje matice inverzní.
v) Ke každé regulární čtvercové matici existuje matice inverzní.
w) Nechť funkce f nabývá v krajních bodech intervalu ⟨□, □⟩ nenulových funkčních hodnot opačných znamének. Pak v intervalu (a, b) existuje aspoň jedno číslo c takové, že $f(c) = 0$.
x) Funkce f je spojitá v intervalu ⟨□, □⟩ právě tehdy, když je v tomto intervalu omezená.

Pouģitá a doporuļená literatura:

[1] BATTY, CH. *How do undergraduates do mathematics*? A guide to studying mathematics at Oxford University, 1994.

[2] BEČVÁŘ, J. a kol. *Seznamujeme se s mnoģinami.* Praha: SNTL, 1982.

[3] EMANOVSKÝ, P., KÜHR, J. *Cviļení z algebry pro 1. roļník I.* Olomouc: VUP, 2007.

[4] FRANKLIN, J., DAOUD, A. *Proof in Mathematics (An Introduction).* Sydney: Quakers Hill Press, 2001.

[5] HORT, D., RACHŮNEK, J. *Algebra I.* Olomouc: VUP, 2005.

[6] HRUŠA, K., DLOUHÝ, Z., ROHLÍČEK, J. – *Úvod do studia matematiky.* Praha: SPN, 1963.

[7] KVĚTOŇ, P. – *Kapitoly z didaktiky matematiky I*, Ostrava: Pedagogická fakulta, 1988. ISBN 80-7042-024-3

[8] KVĚTOŇ, P. – *Cviļení z didaktiky matematiky*, Ostrava: REPRONIS, 2000. ISBN 80-7042-171-1

[9] VELLEMAN, D. J. – *How to prove it.* Cambridge: University Press, 2006.