Úvodní kurs ze základů matematiky

L. Pick (KMA), M. Rokyta (KMA), J. Tůma (KA)

27. září 2012

Obsah

1 Výroky

Univerzitní matematika se od středoškolské matematiky odlišuje především důrazem na *abstrakci* a na *přesnost uvažování*.

Abstrakcí rozumíme to, že se většinou nebudeme zabývat konkrétními čísly nebo funkcemi, ale budeme zkoumat celé třídy matematických objektů, jako jsou čísla, rovnice, funkce, algoritmy, pravidla počítání. Výpočty budeme většinou provádět se symboly jako x, f, A, $\mathbf{v}$, atd.

1.1 Výroková a predikátová logika

Definice 1.1. *Výrok* je dobře zformulované tvrzení, o kterém má smysl říci, zda je pravdivé (platí) nebo není pravdivé (neplatí). Výrokům přisuzujeme *pravdivostní hodnotu*. Pokud výrok platí, říkáme, že má pravdivostní hodnotu 1, pokud neplatí, říkáme, že má pravdivostní hodnotu 0. Věda o formální správnosti výroků se nazývá *logika.*

Příklady.

- Obloha je modrá. (Je výrok.)
- Nový Bydžov je hlavní město Kanady. (Je výrok.)
- Ahoj! (Není výrok.)
- Kéž by už byl konec hodiny! (Není výrok.)
- 2^{π} je iracionální číslo. (Je výrok, i když se neví, zda pravdivý či ne.)

Výroky můžeme kombinovat do složitějších výroků pomocí *logických spojek*.

Definice 1.2. Definujeme následující *logické spojky a operace*:

- *Konjunkcí* $A\&B$ výroků A, B nazveme výrok: *Platí A a zároveň platí B*. Konjunkce se také někdy značí $A \wedge B$.
- *Disjunkcí* $A \vee B$ výroků A a B nazveme výrok: *Platí A nebo B* ve smyslu *platí alespoň jeden z výroků A, B*.
- *Implikací* $A \Rightarrow B$ nazýváme výrok: *Jestliže platí výrok A, potom platí výrok B.*

  Výroku A v implikaci se říká *premisa* (případně *předpoklad*), výrok B se nazývá *závěr* (případně *důsledek*).

  Pokud je výrok $A \Rightarrow B$ pravdivý, pak říkáme, že A je *postačující podmínkou* pro platnost B a B je *nutnou podmínkou* pro platnost A.
- *Ekvivalencí* $A \Leftrightarrow B$ nazýváme výrok: *Výrok A platí tehdy a jen tehdy, když platí výrok B.*

  Říkáme také, že (platnost výroku) A je *nutnou a postačující* podmínkou (platnosti výroku) B.
- *Negací* $\neg A$ (případně non A) výroku A rozumíme výrok: *Není pravda, že platí A.*

Tabulka pravdivostních hodnot:

A	$\neg A$
0	1
1	0

A	B	A & B	A $\vee$ B	A $\Rightarrow$ B	A $\Leftrightarrow$ B
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Poznámky. (1) Logická spojka *nebo* (disjunkce) není *vylučující*, tj. disjunkce je pravdivá i když platí oba výroky A a B.

(2) Je-li premisa implikace A nepravdivá, pak implikace platí vždy bez ohledu na platnost důsledku B (jinými slovy, z nepravdivého výroku plyne cokoli).

Definice 1.3. *Výroková forma* $V(x_1, \dots, x_n)$ (též *výroková funkce* nebo *predikát*) je výraz, z něhož vznikne výrok poté, co do něj dosadíme za proměnné $x_1, \dots, x_n$, prvky z daných množin $A_1, \dots, A_n$.

Příklad. Nechť výroková forma V je dána pro $x \in \{2, 3, 4, 5\}$ předpisem „$x < 3$“. Pak platí $V(2)$, ale neplatí $V(5)$.

Definice 1.4. *Kvantifikátory:*

- velký (též všeobecný) kvantifikátor, značíme $\forall$, čteme „pro každé“;
- malý (též existenční) kvantifikátor, značíme $\exists$, čteme „existuje“.

Příklad. Obecný zápis

$$\forall x \in M\ \exists y \in N\ \forall a, b \in I:\ V(x, y, a, b),$$

čteme „pro každé $x \in M$ existuje $y \in N$ takové, že pro každé $a, b \in I$ platí výrok $V(x, y, a, b)$“. Často se také místo dvojtečky ve výše uvedeném zápise používá středník, tedy lze psát

$$\forall x \in M\ \exists y \in N\ \forall a, b \in I;\ V(x, y, a, b).$$

Poznámka 1.5. Jestliže výrok obsahuje několik po sobě jdoucích kvantifikátorů stejného typu, pak lze jejich pořadí libovolně měnit, například

$$\forall x \in M\ \forall y \in N:\ V(x, y) \ \Leftrightarrow\ \forall y \in N\ \forall x \in M:\ V(x, y).$$

Změníme-li ovšem pořadí kvantifikátorů různého typu, pak se obvykle změní smysl výroku. Výrok

$$\exists x \in M\ \forall y \in N:\ V(x, y)$$

sice implikuje výrok

$$\forall y \in N\ \exists x \in M:\ V(x, y),$$

ale opačná implikace obecně neplatí. Například výrok

$$\forall y \in \mathbb{N}\ \exists x \in \mathbb{N}:\ x > y$$

platí, ale

$$\exists y \in \mathbb{N}\ \forall x \in \mathbb{N}:\ x > y$$

nikoli.

Definice 1.6. Zápis

$$\exists!\ x \in M:\ V(x)$$

čteme„existuje právě jedno $x \in M$, pro které platí výrok $V(x)$“. Příklad:

$$\forall x \geq 0\ \exists!\ y \geq 0:\ y^2 = x.$$

2 Číselné množiny

Intuitivně budeme zacházet s množinami přirozených čísel $\mathbb{N}$, celých čísel $\mathbb{Z}$ a racionálních čísel $\mathbb{Q}$.

V literatuře i v přednáškách se vyskytují dvě různé definice množiny přirozených čísel. Zatímco v matematické analýze pod přirozenými čísly rozumíme množinu $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ a klademe $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, v některých jiných matematických disciplínách (například v diskrétní matematice) je množina přirozených čísel chápána jako množina $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$, nulu je tedy počítána mezi přirozená čísla.

Dále budeme pracovat s množinou celých čísel $\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$ a množinou racionálních čísel $\mathbb{Q} = \{x = \frac{p}{q}; p \in \mathbb{Z}, q \in \mathbb{N}\}$.

Množina reálných čísel $\mathbb{R}$ bude zavedena později na přednášce z matematické analýzy.

2.1 Kongruence celých čísel

V tomto paragrafu číslo 0 za přirozené číslo *nepovažujeme*.

Následující věta se týká dělení se zbytkem.

Věta 2.1. *Je-li $a \in \mathbb{Z}$ a $n \in \mathbb{N}$, pak existují jednoznačně určená čísla $q \in \mathbb{Z}$ a $r \in \{0, 1, \ldots, n-1\}$ taková, že*

$$a = nq + r.$$

Definice 2.2. Číslo $r \in \{0, 1, \ldots, n-1\}$ z předchozí věty nazýváme *zbytek při dělení a číslem n*.

Zbytek při dělení a číslem n označujeme $a \mod n$.

Definice 2.3. Jsou-li $a, b \in \mathbb{Z}$, pak říkáme, že a *dělí* b, jestliže existuje $c \in \mathbb{Z}$ takové, že $b = ac$.

Skutečnost, že a dělí b zapisujeme také $a \mid b$.

Definice 2.4. Jsou-li $a, b \in \mathbb{Z}$ a $n \in \mathbb{N}$, pak říkáme, že a *je kongruentní s b modulo n*, jestliže n dělí $a - b$.

Skutečnost, že a je kongruentní s b modulo n zapisujeme jako $a \equiv b \pmod{n}$. Jestliže a není kongruentní s b modulo n, pak píšeme $a \not\equiv b \pmod{n}$.

Věta 2.5. *Pro libovolná $a, b \in \mathbb{N}$ a pro libovolné $n \in \mathbb{N}$ platí $a \equiv b \pmod{n}$ právě tehdy, když $a \mod n = b \mod n$.*

Věta 2.6. *Buď $a, b, c \in \mathbb{Z}$ a $n \in \mathbb{N}$. Pak platí*

1. *$a \equiv a \pmod{n}$,*
2. *jestliže $a \equiv b \pmod{n}$, pak $b \equiv a \pmod{n}$,*
3. *jestliže $a \equiv b \pmod{n}$ a $b \equiv c \pmod{n}$, pak $a \equiv c \pmod{n}$.*

Věta 2.7. *Buď $a, b, c, d \in \mathbb{Z}$ a $n \in \mathbb{N}$. Pak platí*

1. *jestliže $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $a + c \equiv b + d \pmod{n}$,*
2. *jestliže $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $ac \equiv bd \pmod{n}$.*

Příklad. • Je-li $a \equiv b \pmod{n}$ a $c \in \mathbb{N}$, pak také $a^c \equiv b^c \pmod{n}$.

Definice 2.8. Jsou-li $a, b \in \mathbb{Z}$, taková, že alespoň jedno z nich je nenulové, pak *největší společný dělitel* čísel a, b je největší celé číslo d, které dělí obě čísla a, b.

Přirozené číslo $n \geq 2$ nazýváme *prvočíslem*, jestliže jediná dvě přirozená čísla, která dělí n, jsou 1 a n.

Největšího společného dělitele čísel a, b budeme označovat $\gcd(a, b)$. Existují rozumné důvody proč někdy definujeme i $\gcd(0, 0) = 0$, zde je ale uvádět nebudeme.

Poznámky 2.9. 1. Pro libovolná čísla $a, b \in \mathbb{Z}$ platí $\gcd(a, b) = \gcd(|a|, |b|)$,

2. pro každé číslo $b \in \mathbb{N}$ platí $\gcd(b, 0) = b$.

Podle bodu 1 předcházející poznámky stačí umět počítat největšího společného dělitele pro dvojice nezáporných čísel.

Věta 2.10. *Pro libovolná čísla $a \in \mathbb{N} \cup \{0\}$ a $b \in \mathbb{N}$ platí $\gcd(a, b) = \gcd(b, a \mod b)$.*

Poslední věta vede k algoritmu pro nalezení největšího společného dělitele $\gcd(a, b)$. Tento algoritmus se nazývá *Euklidovým algoritmem*.

Věta 2.11. *Jsou-li $a, b \in \mathbb{Z}$ libovolná čísla, pak existují čísla $s, t \in \mathbb{Z}$ taková, že*

$$\gcd(a, b) = as + bt.$$

Věta 2.12. *Pro každé prvočíslo p a každé celé číslo a, které není násobkem p, existuje číslo $s \in \mathbb{Z}$ takové, že*

$$as \equiv 1 \ (\mod p).$$

Věta 2.13. *Pro každé prvočíslo p a každá čísla $a, b \in \mathbb{Z}$ taková, že a není dělitelné p, existuje číslo $x \in \mathbb{Z}$ takové, že*

$$ax \equiv b \ (\mod p).$$

Platí-li pro $y \in \mathbb{Z}$, že $ax \equiv b \pmod{n}$, pak $x \equiv y \pmod{p}$.

2.2 Komplexní čísla

V tomto oddílu budeme dočasně předpokládat, že již známe množinou reálných čísel, přestože tato množina bude zavedena teprve později.

Definice 2.14. *Množinu komplexních čísel* $\mathbb{C}$ definujeme jako množinu všech uspořádaných dvojic $[a, b]$, kde $a, b \in \mathbb{R}$, přičemž pro komplexní čísla $x = [a, b]$, $y = [c, d]$ definujeme operace *sčítání* a *násobení* takto

- $x + y = [a + c, b + d]$,
- $x \cdot y = [ac - bd, ad + bc]$.

Dále definujeme $0 = [0, 0]$, $1 = [1, 0]$ a $i = [0, 1]$. Pro číslo $x = [a, b] \in \mathbb{C}$ pak platí $x = [a, b] = a[1, 0] + b[0, 1] = a + ib$. Tento zápis komplexního čísla je běžnější.
Nechť $x = [a, b] = a + ib \in \mathbb{C}$.

- Prvek a nazýváme *reálnou částí* x, prvek b nazýváme *imaginární částí* x.
- *Komplexně sdruženým číslem* k x rozumíme číslo $\overline{x} = [a, -b] = a - ib$; symbol $-x$ značí číslo $[-a, -b] = -a - ib$ a symbol $1/x$ značí pro $x \neq 0$ (jednoznačně určené) číslo splňující $x \cdot \frac{1}{x} = 1$.
- *Absolutní hodnotou* komplexního čísla x rozumíme $\sqrt{a^2 + b^2}$.

Poznámka 2.15. Každé číslo $a \in \mathbb{R}$ můžeme ztotožnit s komplexním číslem $[a, 0]$.

3 Základní typy důkazů

- **Přímý důkaz:** Při důkazu výroku $A \Rightarrow B$ vyvozujeme B z A postupnými dedukcemi.

  Při důkazu výroku $\forall\, x \in M \colon V(x)$ lze postupovat takto:

  1. krok: zvolíme $x \in M$ pevné, ale libovolné.

  2. krok: postupnými dedukcemi ukážeme platnost $V(x)$ pro x;
- **Nepřímý důkaz:** Místo $\forall\, x \in M \colon V(x)$ dokážeme $\neg V(x) \Rightarrow x \notin M$. Podobně místo $A \Rightarrow B$ dokážeme $\neg B \Rightarrow \neg A$.
- **Důkaz sporem:** Chceme dokázat $A \Rightarrow B$. Předpokládáme $A \& \neg B$ a najdeme výrok V takový, že z předpokladu $A \& \neg B$ plyne $V \& \neg V$.
- **Důkaz rozborem případů.**
- **Důkaz matematickou indukcí:** Při důkazu tvrzení $\forall\, n \in \mathbb{N} \colon V(n)$

  1. dokážeme nejprve platnost $V(1)$,
  2. poté dokážeme $\forall\, n \in \mathbb{N} \colon [V(n) \Rightarrow V(n + 1)]$.

Poznámka 3.1. Při důkazu výroku $\exists\, x \in M \colon V(x)$ máme dvě možnosti:
buď najdeme nějaké $x_0 \in M$, pro které platí $V(x)$
nebo takové $x_0 \in M$ nenajdeme, ale dokážeme, že alespoň jedno musí existovat.

Příklady.
- Dokažte přímo, nepřímo a sporem následující tvrzení: je-li $n \in \mathbb{N}$ a n^2 je liché, pak také n je liché.
- Dokažte matematickou indukcí, že každé $n \in \mathbb{N}$ lze zapsat buď ve tvaru $2k$ nebo ve tvaru $2k - 1$ pro nějaké $k \in \mathbb{N}$.
- Dokažte sporem, že neexistuje žádné racionální číslo x splňující $x^2 = 2$.

4 Množiny a množinové operace

Pracujeme v tzv. Zermelo-Frankelově teorii množin dané systémem axiomů. Detaily této teorie sahají hluboko za rámec tohoto textu a nebudou zde uvedeny. S objekty teorie množin pracujeme intuitivním způsobem. Budeme vycházet z toho, že každá množina je určena svými prvky.

Značení 4.1. Budeme používat standardní množinové operace a standardní značení: jsou-li A a B množiny, pak

- $A = B$ (A *rovná se* B), pokud mají stejné prvky, v opačném případě píšeme $A \neq B$;
- $A \subset B$ nebo $A \subseteq B$ znamená, že množina A je *podmnožinou* množiny B, tj. $[\forall x \in A\colon\ x \in B]$;
- $A \subsetneq B$ znamená, že množina A je podmnožinou množiny B a přitom $A \neq B$; říkáme, že A je *vlastní podmnožinou* B;
- *prázdnou množinou* nazveme množinu neobsahující žádný prvek a značíme ji $\emptyset$;
- je-li $V(x)$ výroková forma a A je množina, pak $B = \{x \in A\colon V(x)\}$ značí množinu těch prvků x z A, které splňují $V(x)$;
- $A \cap B = \{x;\ x \in A\ \&\ x \in B\}$ je *průnik* množin A a B;
- obecněji, je-li $I \neq \emptyset$ a A_i, $i \in I$, jsou množiny, pak $\bigcap\limits_{i\in I} A_i = \{x; \forall\, i \in I\colon x \in A_i\}$;
- $A \cup B = \{x;\ x \in A\ \vee\ x \in B\}$ je *sjednocení* množin A a B;
- obecněji, je-li $I \neq \emptyset$ a A_i, $i \in I$, jsou množiny, pak $\bigcup\limits_{i\in I} A_i = \{x; \exists\, i \in I\colon x \in A_i\}$;
- jestliže $A \cap B = \emptyset$, řekneme, že A, B jsou *disjunktní* množiny;
- $A \setminus B = \{x \in A;\ x \notin B\}$ je *rozdíl* množin A a B;
- *symetrický rozdíl* $A \div B$ množin A a B definujeme předpisem

$$A \div B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Věta 4.2 (de Morganova pravidla)**.** *Nechť X a I jsou množiny, $I \neq \emptyset$, a nechť A_i, $i \in I$, jsou množiny. Pak*

$$X \setminus \bigcup_{i\in I} A_i = \bigcap_{i\in I} (X \setminus A_i) \quad a \quad X \setminus \bigcap_{i\in I} A_i = \bigcup_{i\in I} (X \setminus A_i)\,.$$

Definice 4.3. Nechť X je množina. Množinu $\{A; A \subset X\}$ nazýváme *potenční množinou množiny* X (nebo *potencí množiny* X) a značíme ji $\exp X$. V literatuře se vyskytují různá další označení pro potenční množinu, například 2^X nebo $P(X)$.

Definice 4.4. Nechť $A_1, \ldots, A_n$ jsou množiny.

- Jejich *kartézským součinem* rozumíme množinu

$$A_1 \times \cdots \times A_n = \{[a_1, \ldots, a_n];\ \forall\, i \in \{1, \ldots, n\}\colon a_i \in A_i\},$$

  tedy množinu uspořádaných n-tic $[a_1, \ldots, a_n]$.

- *Binární relací* R mezi množinami A a B rozumíme libovolnou podmnožinu kartézského součinu $A \times B$. Často také hovoříme o *relaci mezi A a B* nebo o *relaci z A do B*. Příslušnost uspořádané dvojice $[a, b]$ do relace R značíme $[a, b] \in R$ nebo aRb.

Definice 4.5. Nechť A a B jsou množiny a nechť $M \subset A \times B$ je binární relace. Pak relaci $M^{-1} \subset B \times A$ definovanou předpisem $[x, y] \in M^{-1} \Leftrightarrow [y, x] \in M$ nazýváme *inverzní relací* k relaci M.

Definice 4.6. Nechť A je množina a nechť $M \subset A \times A$ je binární relace. Řekneme, že M je

- *reflexivní*, jestliže $\forall x \in A\colon\ [x,x] \in M$,
- *symetrická*, jestliže $\forall x,y \in A,\ [x,y] \in M\colon\ [y,x] \in M$,
- *tranzitivní*, jestliže $\forall x,y,z \in A,\ [x,y] \in M,\ [y,z] \in M\colon\ [x,z] \in M$,
- *antireflexivní*, jestliže $\forall x \in A\colon\ [x,x] \notin M$,
- *antisymetrická*, jestliže $\forall x,y \in A, [x,y] \in M, :\ [y,x] \notin M$,
- *slabě antisymetrická*, jestliže $\forall x,y \in A,\ [x,y] \in M,\ [y,x] \in M\colon\ x = y$.

Definice 4.7. Nechť A je množina a nechť $M \subset A \times A$ je binární relace. Řekneme, že M je

- *ekvivalence*, jestliže je reflexivní, symetrická a tranzitivní;
- *částečné uspořádání* (někdy jen *uspořádání* či *neostré uspořádání*), jestliže je reflexivní, slabě antisymetrická a tranzitivní;
- *ostré uspořádání*, jestliže je antireflexivní, antisymetrická a tranzitivní;
- *lineární uspořádání*, jestliže je to částečné uspořádání a pro každé dva prvky $x, y \in A$ nastává buď $[x,y] \in M$ nebo $[y,x] \in M$.

5 Zobrazení a funkce

Definice 5.1. Binární relaci $F \subset A \times B$ nazýváme *zobrazením* neboli *funkcí* množiny A do množiny B (a zpravidla značíme $F : A \to B$), jestliže platí

$$\forall x \in A\ \forall y_1, y_2 \in B\colon\ (([x,y_1] \in F\ \&\ [x,y_2] \in F) \Rightarrow (y_1 = y_2)).$$

Množinu

$$\{x \in A;\ \exists y \in B\colon\ [x,y] \in F\}$$

nazýváme *definičním oborem* zobrazení (funkce) F a značíme $D(F)$ (nebo $\mathrm{Dom}(F)$). Množinu

$$\{y \in B;\ \exists x \in A\colon\ [x,y] \in F\}$$

nazýváme *oborem hodnot* a značíme $H(F)$ (nebo $R(F)$ nebo $\mathrm{Rng}(F)$). Místo $[x,y] \in F$ obvykle píšeme $F(x) = y$.

Jsou-li A, B množiny a $F \subset A \times B$ je zobrazení, pak tento fakt značíme symbolem $F : A \to B$.

Poznámka. Zobrazení není totéž co předpis, neboť různé předpisy mohou definovat stejné zobrazení. Například zobrazení $f : \mathbb{R} \to \mathbb{R}$ a $g : \mathbb{R} \to \mathbb{R}$, definovaná pomocí předpisů

$$f(x) = \sqrt{x^2 + 2x + 1}, \qquad g(x) = |x + 1|, \quad x \in \mathbb{R},$$

splňují $f = g$.

Definice 5.2. Nechť A a B jsou množiny a nechť $f : A \to B$ je zobrazení.

- Nechť $M \subset A$. Pak množinu

  $$f(M) = \{y \in B;\ \exists x \in M\colon\ f(x) = y\}$$

  nazýváme *obrazem množiny* M při zobrazení f.
- Nechť P je libovolná množina. Pak množinu

  $$f^{-1}(P) = \{x \in A;\ f(x) \in P\}$$

  nazýváme *vzorem množiny* P při zobrazení f.

Definice 5.3. Nechť A a B jsou množiny a nechť $f : A \to B$ je zobrazení.

(1) Řekneme, že f je *prosté* (*injektivní*), jestliže

$$\forall x, y \in A\colon\ (f(x) = f(y)\ \Rightarrow\ x = y).$$

(2) Řekneme, že f je „*na*“ (*surjektivní*), jestliže

$$\forall y \in B\ \exists x \in A\colon\ f(x) = y.$$

(3) Řekneme, že f je *bijekce* (*vzájemně jednoznačné*), jestliže je zároveň prosté a „na“.

Poznámka. Abychom mohli říci, zda nějaké zobrazení je „na“, musí být přesně zadána koncová množina B (takže (2) a (3) můžeme chápat jako vlastnosti zobrazení f a množiny B).

Definice 5.4.

- Nechť A a B jsou množiny, nechť $f : A \to B$ je zobrazení a nechť $C \subset A$. Pak zobrazení $g : C \to B$ definované předpisem

$$g(x) = f(x), \quad x \in C,$$

(značíme $g = f|_C$) nazýváme *restrikcí* (*zúžením* nebo *parcializací*) zobrazení f na množinu C.

- Nechť A, B, C jsou množiny a nechť $f : A \to B$, $g : B \to C$ jsou zobrazení. Pak zobrazení $g \circ f : A \to C$ definované předpisem

$$(g \circ f)(x) = g(f(x)), \quad x \in A,$$

nazýváme *složeným zobrazením* (*složením zobrazení f a g*), přičemž g nazýváme *vnějším* zobrazením a f nazýváme *vnitřním* zobrazením.

Poznámka. Skládání zobrazení je asociativní operace, ale není komutativní (cvičení).

Definice 5.5. Nechť A a B jsou množiny a nechť $f : A \to B$ je prosté. Pak zobrazení $f^{-1} : f(A) \to A$ definované předpisem

$$f^{-1}(y) = x \quad \Leftrightarrow \quad y = f(x), \quad x \in A,\ y \in f(A),$$

nazýváme *inverzním zobrazením* k zobrazení f.

Poznámka. K neprostému zobrazení nelze definovat inverzní zobrazení. Lze definovat pouze inverzní binární relaci, která ale nebude zobrazením. Příkladem je funkce $f : \mathbb{R} \to [0, \infty)$, definovaná předpisem $f(x) = x^2$ pro $x \in \mathbb{R}$. (V tomto příkladu pracujeme intuitivně s intervalem reálných čísel, přestože ten bude zaveden teprve později.)

6 Mohutnosti množin

Definice 6.1.

- Říkáme, že množiny A, B *mají stejnou mohutnost*, jestliže existuje bijekce A na B, píšeme $A \approx B$;

- Říkáme, že množina A *má mohutnost menší nebo rovnou mohutnosti množiny* B, jestliže existuje prosté zobrazení A do B. Píšeme $A \preceq B$; relaci „$\preceq$“ říkáme *subvalence*.

Definice 6.2. Řekneme, že množina X je *nekonečná*, jestliže má stejnou mohutnost jako nějaká její vlastní podmnožina. V opačném případě říkáme, že X je *konečná*. Řekneme, že množina X je *spočetná*, jestliže je konečná nebo má stejnou mohutnost jako $\mathbb{N}$. Nekonečná množina, která není spočetná, se zove *nespočetná*.

Poznámka. Pro počet prvků konečné množiny X používáme často značení $|X|$. Dvě konečné množiny X, Y mají stejnou mohutnost právě tehdy, když $|X| = |Y|$.

Věta 6.3 (Cantor–Bernstein)**.** *Nechť A, B jsou množiny takové, že A má mohutnost menší nebo rovnu než B a B má mohutnost menší nebo rovnu než A. Pak mají stejnou mohutnost.*

Věta 6.4 (Cantor)**.** *Nechť X je množina. Pak neexistuje zobrazení $\varphi : X \to \exp X$, které je „na“.*

7 Cvičení

7.1 K výrokům

Cvičení 1. Negujte výroky

$$\forall\, x \in M\colon V(x);$$
$$\exists\, x \in M\colon V(x);$$
$$\exists\, x \in M\ \forall\, y \in M\colon W(x,y);$$
$$\exists\, y \in M\ \forall\, x \in M\colon W(x,y).$$

Cvičení 2. Nechť M je množina osob přítomných v posluchárně a nechť $W(x,y)$ znamená: osoba x zná příjmení osoby y. Zkoumejte platnost výroků

$$\forall\, x \in M\ \exists\, y \in M\colon W(x,y);$$
$$\forall\, y \in M\ \exists\, x \in M\colon W(x,y);$$
$$\exists\, x \in M\ \forall\, y \in M\colon W(x,y);$$
$$\exists\, y \in M\ \forall\, x \in M\colon W(x,y).$$

Cvičení 3. Platí

$$\neg\left(\forall\, x \in \mathbb{R}\ \exists\, y \in \mathbb{R}\ \forall\, z \in \mathbb{R}\colon (z > y \Rightarrow z > x)\right) \quad \Leftrightarrow \quad \left(\exists\, x \in \mathbb{R}\ \forall\, y \in \mathbb{R}\ \exists\, z \in \mathbb{R}\colon (z > y\ \&\ z \leq x)\right).$$

Cvičení 4. Platí:

$$\begin{aligned}
\neg(\forall\, x \in M\colon V(x)) &\quad \Leftrightarrow \quad \exists\, x \in M\colon \neg V(x);\\
\neg(\exists\, x \in M\colon V(x)) &\quad \Leftrightarrow \quad \forall\, x \in M\colon \neg V(x);\\
\neg(\forall\, x \in M\colon A(x) \Rightarrow B(x)) &\quad \Leftrightarrow \quad \exists\, x \in M\colon A(x)\&\neg B(x).
\end{aligned}$$

Cvičení 5. Znegujte výrok: Každý si rád dá jedno pivo, ale ne vždy a ne v každé hospodě.

7.2 Ke kongruenci

Cvičení 7.1. *Najděte poslední cifru čísla* 3^{991}.

7.3 K důkazové technice

Cvičení 6.

- Existují dvě iracionální čísla x, y taková, že $x^y \in \mathbb{Q}$.
- Existují dvě osoby v této posluchárně, které mají narozeniny ve stejném týdnu.
- Existují dvě ženy v Praze, které mají stejný počet vlasů.

Cvičení 7. Pro $n \in \mathbb{N}$ je číslo $\sqrt{n}$ buď celé nebo již iracionální.

Cvičení 8. (Bernoulli) Nechť $x \in \mathbb{R}$, $x \geq -1$, $n \in \mathbb{N}$. Pak platí Bernoulliova nerovnost

$$(1+x)^n \geq 1 + nx.$$

Dokažte matematickou indukcí. Indukcí s krokem „$n \to n{+}2$“ dále ukažte, že uvedená nerovnost platí i pro $x \geq -2$. Ukažte na příkladě, že pro $x < -2$ a obecné $n \in \mathbb{N}$ již Bernoulliova nerovnost neplatí.

Cvičení 9. Dodatek*: (zobecněná Bernoulliho nerovnost) Ukažte: Nechť $n \in \mathbb{N}$. Platí-li pro všechna $k \in \{1, 2, \ldots, n\}$ buď $x_k \geq 0$ nebo $0 \geq x_k \geq -2$, je

$$(1+x_1)(1+x_2)\ldots(1+x_n) \geq 1 + x_1 + \cdots + x_n\,.$$

Cvičení 10. (Cauchy) Nechť $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ jsou reálná čísla. Potom platí

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right).$$

Cvičení 11. (AG nerovnost) Nechť $a_1, \ldots, a_n$ jsou nezáporná reálná čísla. Pak platí

$$\frac{\sum_{i=1}^n a_i}{n} \geq \sqrt[n]{\prod_{i=1}^n a_i}.$$

Ukažte, že rovnost v AG nerovnosti platí právě tehdy, když $a_1 = a_2 = \cdots = a_n$. Ukažte, že pro kladná reálná čísla $a_1, \ldots, a_n$ platí tzv. AGH nerovnost

$$\frac{\sum_{i=1}^n a_i}{n} \geq \sqrt[n]{\prod_{i=1}^n a_i} \geq \frac{n}{\sum_{i=1}^n \frac{1}{a_i}}$$

přičemž i zde rovnosti platí právě tehdy, když $a_1 = a_2 = \cdots = a_n$.

7.4 Binárni relace a zobrazení

Cvičení 12. Nerovnost mezi reálnými čísly „$\leq$“ tvoří binární relaci na $[0, 1]$. Tuto relaci lze také graficky znázornit pomocí horního trojúhelníku ve čtverci $[0, 1]^2$.

Cvičení 13. Jakákoli výroková funkce $V(x, y)$ na $A \times B$ vytváří binární relaci $M = \{[x, y] \subset A \times B;\ V(x, y)\}$ a naopak.

Cvičení 14. Inverzní relací k relaci „$\leq$“ na $[0, 1]^2$ je relace „$\geq$“.

Cvičení 15.

- Nechť A je libovolná neprázdná množina. Pak relace *rovnost* $(=)$ je ekvivalence na A.
- Nechť $p \in \mathbb{N}$. Pak relace *kongruence modulo p* definovaná předpisem

  $$m \equiv n \pmod p \quad \Leftrightarrow \quad |m - n| \text{ je dělitelné číslem } p,$$

  je ekvivalence na $\mathbb{N}$.
- Relace menší nebo rovno než $(\leq)$ je lineární uspořádání na $\mathbb{R}$.
- Nechť A je množina všech funkcí z intervalu $[0, 1]$ do $\mathbb{R}$ a nechť $\leq$ je relace definovaná předpisem

  $$f \leq g \ \Leftrightarrow\ \forall\, x \in [0, 1] :\ f(x) \leq g(x).$$

  Pak $\leq$ tvoří na množině A částečné uspořádání, které není lineární.
- Je-li X množina, pak relace

  $$R = \{[A, B] \in \exp X \times \exp X; A \subset B\}$$

  je částečné uspořádání na $\exp X$, které obecně není lineární.

Cvičení 16. Nechť A a B jsou množiny a nechť $f : A \to B$ je zobrazení. Pak

- f je prosté právě tehdy, když rovnice $f(x) = y$ má pro každé $y \in B$ nejvýše jedno řešení;
- f je „na“ právě tehdy, když rovnice $f(x) = y$ má pro každé $y \in B$ alespoň jedno řešení;
- f je bijekce právě tehdy, když rovnice $f(x) = y$ má pro každé $y \in B$ právě jedno řešení.

Cvičení 17. Necht $f : A \to C$ a $g : A \to B$ splňují $g(A) = B$. Najděte nutnou a postačující podmínku pro existenci zobrazení $h : B \to C$ splňujícího $f = h \circ g$.

Cvičení 18. Absolutní hodnota splňuje takzvanou *trojúhelníkovou nerovnost*:

$$\forall\, x, y, z \in \mathbb{C}\colon |x - y| \leq |x - z| + |z - y|.$$

Cvičení 19. Nechť $A_n \subset \mathbb{C}$, $n \in \mathbb{N}$, jsou množiny. Pak platí

$$\{z \in \mathbb{C}; \{n \in \mathbb{N}; z \notin A_n\} \text{ je konečná}\} = \bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} A_k,$$

$$\{z \in \mathbb{C}; \{n \in \mathbb{N}; z \in A_n\} \text{ není konečná}\} = \bigcap_{n=1}^{\infty} \bigcup_{k=n}^{\infty} A_k.$$

Cvičení 20. Nechť $f\colon \mathbb{N} \to \mathbb{N}$. Rozhodněte o platnosti následujících tvrzení:

- Je-li $f(\mathbb{N})$ konečná, není f prosté.
- Je-li $f(\mathbb{N})$ nekonečná, je f prosté.
- Je-li $\mathbb{N} \setminus f(\mathbb{N}) = \emptyset$, je f prosté.
- Je-li f prosté, je $\mathbb{N} \setminus f(\mathbb{N}) = \emptyset$.

Cvičení 21. Uvažujme zobrazení $f : X \to Y$ a množiny $A \subset X$, $B \subset X$. Dokažte následující rovnosti.

- $f(A \cup B) = f(A) \cup f(B)$,
- $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$,
- $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$,
- $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

Cvičení 22. Uvažujme zobrazení $f : X \to Y$ a množiny $A \subset X$, $B \subset X$. Ukažte, že následující vztahy obecně neplatí.

- $f(A \cap B) = f(A) \cap f(B)$,
- $f(A \setminus B) = f(A) \setminus f(B)$.

Cvičení 23. Ukažte, že bez ohledu na pravdivostní hodnotu výroků A, B, C jsou následující výroky vždy pravdivé.

- $A \;\&\; (B \;\&\; C) \Leftrightarrow (A \;\&\; B) \;\&\; C$,
- $A \;\&\; (B \vee C) \Leftrightarrow (A \;\&\; B) \vee (A \;\&\; C)$,
- $A \vee (B \;\&\; C) \Leftrightarrow (A \vee B) \;\&\; (A \vee C)$,
- $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$,
- $\neg(A \Rightarrow B) \Leftrightarrow (A \;\&\; \neg B)$.

7.5 K mohutnosti množin

Cvičení 24. Ukažte, že počet všech podmnožin množiny $\{1, \ldots, n\}$ je 2^n.

Cvičení 25. Buď X konečná množina, $|X| = n \in \mathbb{N}$. Označme pro $k \in \mathbb{N} \cup \{0\}$, $k \leq n$,

$$\binom{X}{k} = \{A \subseteq X;\, |A| = k\}.$$

Potom platí

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}.$$

Cvičení 26.

- Je-li A neprázdná množina, je A konečná právě tehdy, když existuje $n \in \mathbb{N}$ tak, že A má stejnou mohutnost jako $\{1, \ldots, n\}$.

- Množiny $\mathbb{N}$ a $\mathbb{N} \times \mathbb{N}$ jsou spočetné. Jakákoli nekonečná podmnožina $\mathbb{N}$ je také spočetná.
- Množina racionálních čísel $\mathbb{Q}$ je spočetná.
- Množiny $\mathbb{R}$, $\exp \mathbb{N}$ jsou nespočetné. Navíc mají tyto množiny stejnou mohutnost.

Cvičení 27. Nechť množiny A_n, $n \in \mathbb{N}$, jsou spočetné. Pak $\bigcup_{n=1}^{\infty} A_n$ je spočetná.

Cvičení 28. Ukažte, že množina $\mathbb{Q}$ je spočetná.

Cvičení 29. Nechť množiny A, B jsou spočetné. Pak $A \times B$ je spočetná.

Cvičení 30. Každá nekonečná podmnožina spočetné množiny má stejnou mohutnost jako $\mathbb{N}$.

Cvičení 31. Množina všech zobrazení z $\mathbb{N}$ do $\{0, 1\}$ je nespočetná.

Cvičení 32. (vlastnosti subvalence) Pro libovolné množiny A, B, C platí:

- $(A \preceq B \ \& \ B \preceq C) \Rightarrow A \preceq C$,
- $A \preceq A$,
- $(A \preceq B \ \& \ B \preceq A) \Rightarrow A \approx B$ (bez důkazu).

Cvičení 33. (vlastnosti ekvivalence mohutnosti množin) Pro libovolné množiny A, B, C platí:

- $A \approx A$ (reflexivita),
- $A \approx B \Rightarrow B \approx A$ (symetrie),
- $(A \approx B \ \& \ B \approx C) \Rightarrow A \approx C$ (tranzitivita).