Teorie množin

pro fajnšmekry - TeMno

Lenka Macálková

BR Solutions 2010 - Orličky

23.2. – 27.2.2010

Bylo nebylo . . .

- Starověké Řecko - nekonečnost nepochopená (úsečka vs. přímka)
- 15. stol. - Mikuláš Kusánský - představa o nekonečném vesmíru
- 1638 - otázka porovnávání nekonečných systémů dle velikosti - Galileo Galilei
- 20. léta 19. století - Leibnitz, Newton, Cauchy - nekonečně malé veličiny a limita
- 50. léta 19. století - Bernard Bolzano a Paradoxy nekonečna
- 70. léta 19. století - Georg Cantor - zakladatel teorie množin, důkaz existence dvou neekvivalentních nekonečných množin

Co bylo dál?

Problémy s Cantorovou naivní teorií množin - antimonie:

- Zermelova: Množina všech množin, které nejsou svým vlastním prvkem
- Russelův paradox holiče: Holič (voják) dostal rozkaz holit jen ty vojáky své čety, kteří se sami neholí, a nesmí holit nikoho jiného
- Berryho: Buď *k* nejmenší přirozené číslo, které nelze definovat českou větou o nejvýše dvaceti slovech.

3. krize matematiky - východiskem je axiomatická výstavba (Zermel, Gödel)

Nějaké pojmy na začátek

Definice

Množinou rozumíme libovolně, jednoznačně vymezený souhrn nějakých objektů. Tyto objekty nazýváme prvky množiny.

Nějaké pojmy na začátek

Definice

Množinou rozumíme libovolně, jednoznačně vymezený souhrn nějakých objektů. Tyto objekty nazýváme prvky množiny.

- extenzionalita: $A = B \Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B)$
- prázdná množina: $\emptyset$ - množina, která nemá žádné prvky
- konečná vs. nekonečná množina
- množinová inkluze a podmnožiny

Sjednocení, průnik a rozdíl

Buď $I \neq \emptyset$ libovolná (tzv. indexová) množina. Buď A_i množina pro každé $i \in I$.

- Sjednocením množin A_i, $i \in I$ nazýváme množinu

$$\bigcup_{i \in I} A_i = \{x; \exists i_0 \in I : x \in A_{i_0}\}.$$

- Průnikem množin A_i, $i \in I$ nazýváme množinu

$$\bigcap_{i \in I} A_i = \{x; \forall i \in I : x \in A_i\}.$$

Ještě si řekneme, co pro nás znamená rozdíl množin A, B:

- $A - B = \{x; x \in A \wedge x \notin B\}$

Kartézský součin

Definice

Kartézským součinem množin A, B rozumíme množinu

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

Kartézský součin

Definice

Kartézským součinem množin A, B rozumíme množinu

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

- POZOR! Kartézský součin není komutativní!
- Kartézská mocnina je zavedena analogickým způsobem jako $\underbrace{A \times A \times \ldots \times A}_{n-\text{krát}}$

Definice

Nechť A, B jsou množiny. Pak libovolná podmnožina ϱ kartézského součinu $A \times B$ se nazývá relace mezi množinami A a B. Je-li $(x, y) \in \varrho$, říkáme, že prvek x je v relaci ρ s prvkem y, často zapisujeme $x \varrho y$. Pokud uvážíme součin $A \times A$, říkáme, že se jedná o relaci na množině A.

Relace a zase relace

Definice

Nechť A, B jsou množiny. Pak libovolná podmnožina ϱ kartézského součinu $A \times B$ se nazývá relace mezi množinami A a B. Je-li $(x, y) \in \varrho$, říkáme, že prvek x je v relaci ρ s prvkem y, často zapisujeme $x\varrho y$. Pokud uvážíme součin $A \times A$, říkáme, že se jedná o relaci na množině A.

Jaká může být relace ϱ na množině A?

- reflexivní: $\forall a \in A$ platí, že $a\varrho a$
- symetrická: pokud $a\varrho b$ pak i $b\varrho a$
- antisymetrická: jestliže $a\varrho b \wedge b\varrho a$, pak $a = b$
- tranzitivní: jestliže $a\varrho b \wedge b\varrho c$, pak $a\varrho c$
- úplná: platí buď $a\varrho b$ nebo $b\varrho a$

Ještě jednou relace

M	ϱ	R	S	A	T	Ú
$\{a, b, c, d\}$	$\{(a,b),(b,a),(b,b),(b,c)\}$	N	N	N	N	N
neprázdná	$\emptyset$	N	A	A	A	N
neprázdná	$M \times M$	A	A	*	A	N
neprázdná	$\{(x,x), x \in M\}$	A	A	A	A	*
$\mathcal{P}(A)$	$\{(X,Y), X, Y \in \mathcal{P}(A) \wedge X \subseteq Y\}$	A	**	A	A	***
$\mathbb{N}$	$\{(a,b), a, b \in \mathbb{N} \wedge a \mid b\}$	A	A	A	A	N
$\mathbb{Z}$	$\{(a,b), a, b \in \mathbb{Z} \wedge a \equiv b (\mathrm{mod}\ m)\}$	N	A	N	A	N

$*$ - je-li M jednoprvková, tak ano

$**$ - je-li A prázdná, tak ano

$***$ - je-li A prázdná nebo jednoprvková, tak ano

Zobrazení

Definice

Uvedeme dvě definice zobrazení:

- Nechť A, B jsou libovolné množiny. Předpis f, který každému prvku množiny A přiřazuje právě jeden prvek množiny B, se nazývá zobrazení množiny A do množiny B, ozn. $f : A \rightarrow B$
- Nechť A, B jsou množiny a nechť f je relace mezi množinami A, B splňující podmínku: ke každému $a \in A$ existuje prrávě jedno $y \in B$ tak, že platí xfy. Pak uspřádanou trojici (A, B, f) nazýváme zobrazením množiny A do množiny B.

První z nich není až tak úplně matematicky korektní, problém dělá pojem "předpis".

Zobrazení

Někdy bychom chtěli, aby zobrazení mělo nějaké pěkné vlastnosti, protože díky nim se pak dostaneme k velmi zajímavým věcem. Nyní uvažme zobrazení $f : A \rightarrow B$, $f(a) = b \; \forall a \in A$. Prvku a se říká vzor a prvku b obraz prvku a.

Zobrazení

Někdy bychom chtěli, aby zobrazení mělo nějaké pěkné vlastnosti, protože díky nim se pak dostaneme k velmi zajímavým věcem. Nyní uvažme zobrazení $f : A \to B$, $f(a) = b \; \forall a \in A$. Prvku a se říká vzor a prvku b obraz prvku a.

- injektivní: každé dva různé prvky množiny A se vždy zobrazí na dva různé prvky množiny B
- surjektivní: na každý prvek množiny B se vždy zobrazí nějaký prvek množiny A
- bijektivní: injektivní a surjektivní zároveň

Zobrazení

Někdy bychom chtěli, aby zobrazení mělo nějaké pěkné vlastnosti, protože díky nim se pak dostaneme k velmi zajímavým věcem. Nyní uvažme zobrazení $f : A \to B$, $f(a) = b \; \forall a \in A$. Prvku a se říká vzor a prvku b obraz prvku a.

- injektivní: každé dva různé prvky množiny A se vždy zobrazí na dva různé prvky množiny B
- surjektivní: na každý prvek množiny B se vždy zobrazí nějaký prvek množiny A
- bijektivní: injektivní a surjektivní zároveň

Pokud je zobrazení bijektivní, můžeme sestrojit zobrazení $f^{-1} : B \to A$, pro každé $b \in B$ je $f^{-1}(b) = a$, kde pro a platí $f(a) = b$.

Skládání zobrazení

Můžu nějak dávat do kopy zobrazení? Není problém! Říká se tomu skládání:

- Nechť $f : A \to B$, $g : B \to C$ jsou zobrazení množin. Potom zobrazení $(g \circ f) : A \to C$ dané předpisem $(g \circ f)(a) = g(f(a))$, $\forall a \in A$ se nazývá složené zobrazení g po f.

POZOR! Skládání zobrazení není komutativní!

Uspořádáné množiny

Definice

Nechť M s relací ϱ, která je reflexivní, antisymetrická a tranzitivní. Pak se relace ϱ nazývá uspořádání a M se nazývá uspořádaná množina. Pokud je uspořádání navíc úplné (tj. každé dva prvky jsou srovnatelné), nazývá se M řetězec nebo lineárně uspořádaná množina

Uspořádané množiny

Definice

Nechť M s relací ϱ, která je reflexivní, antisymetrická a tranzitivní. Pak se relace ϱ nazývá uspořádání a M se nazývá uspořádaná množina. Pokud je uspořádání navíc úplné (tj. každé dva prvky jsou srovnatelné), nazývá se M řetězec nebo lineárně uspořádaná množina

Relaci uspořádání si obvykle označujeme $\leq$ nebo $\subseteq$, ale není to vysloveně pravidlem

Uspořádáné množiny

Definice

Nechť M s relací ϱ, která je reflexivní, antisymetrická a tranzitivní. Pak se relace ϱ nazývá uspořádání a M se nazývá uspořádaná množina. Pokud je uspořádání navíc úplné (tj. každé dva prvky jsou srovnatelné), nazývá se M řetězec nebo lineárně uspořádaná množina

Relaci uspořádání si obvykle označujeme $\leq$ nebo $\subseteq$, ale není to vysloveně pravidlem

Příklady:

- Množina $(\mathcal{P}(A), \subseteq)$ je uspořádaná. Pokud je $A = \emptyset$ nebo je A jednoprvková, je dokonce lineárně uspořádaná
- Množina $(\mathbb{N}, |)$ je uspořádaná, ale $(\mathbb{Z}, |)$ uspořádaná není

Uspořádané množiny a izomorfismus

V uspořádaných množinách mají některé prvky "zajímavé" postavení:

- nejmenší (největší) prvek a: $\forall x \in M$ platí $a \leq x$ ($x \leq a$)
- minimální (maximální) prvek a: $\nexists\, x \in M$: $x < a$ ($a < x$)

Uspořádané množiny a izomorfismus

V uspořádaných množinách mají některé prvky "zajímavé" postavení:

- nejmenší (největší) prvek a: $\forall x \in M$ platí $a \leq x$ ($x \leq a$)
- minimální (maximální) prvek a: $\nexists\, x \in M$: $x < a$ ($a < x$)

Izomorfismus

Nechť A, B jsou uspořádané množiny. Zobrazení $f : A \to B$ se nazývá izomorfismem množin A, B, jestliže je bijektivní, zachovává uspořádání a f^{-1} rovněž zachovává uspořádání (tomu se říká, že je izotonní). Množiny A, B pak nazýváme izomorfní a píšeme $A \cong B$.

Uspořádané množiny a izomorfismus

V uspořádaných množinách mají některé prvky "zajímavé" postavení:

- nejmenší (největší) prvek a: $\forall x \in M$ platí $a \leq x$ ($x \leq a$)
- minimální (maximální) prvek a: $\nexists\, x \in M$: $x < a$ ($a < x$)

Izomorfismus

Nechť A, B jsou uspořádané množiny. Zobrazení $f : A \to B$ se nazývá izomorfismem množin A, B, jestliže je bijektivní, zachovává uspořádání a f^{-1} rovněž zachovává uspořádání (tomu se říká, že je izotonní). Množiny A, B pak nazýváme izomorfní a píšeme $A \cong B$.

Příklady:

- $f : (\mathbb{N}, |) \longrightarrow (\mathbb{N}, \leq)$ není izomorfismus, neboť f^{-1} není izotonní
- $f : (\mathbb{N}, \leq) \longrightarrow (2\mathbb{N}, \leq)$ je izomorfismus

Dobře uspořádané množiny

Definice

Uspořádaná množina se nazývá dobře uspořádaná, jestliže každá její neprázdná podmnožina má nejmenší prvek

Dobře uspořádané množiny

Definice

Uspořádaná množina se nazývá dobře uspořádaná, jestliže každá její neprázdná podmnožina má nejmenší prvek

Vlastnosti dobře uspořádané množiny A

- A je řetězec.
- je-li $A \neq \emptyset$, pak A obsahuje nejmenší prvek
- je-li $B \subseteq A$, pak B je dobře uspořádaná
- je-li $A \cong B$, pak je B dobře uspořádaná
- není-li x největší v A, pak v A existuje bezprostřední následník x

Dobře uspořádané množiny

Věta

Řetězec je dobře uspořádaný právě tehdy, když každý jeho klesající řetězec je konečný.

Dobře uspořádané množiny

Věta

Řetězec je dobře uspořádaný právě tehdy, když každý jeho klesající řetězec je konečný.

Důkaz

"$\Leftarrow$" $\emptyset \neq B \subseteq A$ lib. Nechť $x_1 \in B$ lib. Pokud je x_1 nejmenší, tak je B DUM. Pokud ne, pak $\exists x_2 < x_1$, neboť A je řetězec. Pokračujeme analogicky. Protože každý podřetězec je konečný, je B DUM.
"$\Rightarrow$" Nechť v A existuje nekonečný klesající řetězec $x_1 > x_2 > \ldots > x_n > \ldots$ Pak množina $\{x_1, x_2, \ldots, x_n, \ldots\}$ nemá nejmenší prvek, tedy A by nebyla DUM.

Dobře uspořádané množiny

Věta

Řetězec je dobře uspořádaný právě tehdy, když každý jeho klesající řetězec je konečný.

Důkaz

"$\Leftarrow$" $\emptyset \neq B \subseteq A$ lib. Nechť $x_1 \in B$ lib. Pokud je x_1 nejmenší, tak je B DUM. Pokud ne, pak $\exists x_2 < x_1$, neboť A je řetězec. Pokračujeme analogicky. Protože každý podřetězec je konečný, je B DUM.
"$\Rightarrow$" Nechť v A existuje nekonečný klesající řetězec $x_1 > x_2 > \ldots > x_n > \ldots$ Pak množina $\{x_1, x_2, \ldots, x_n, \ldots\}$ nemá nejmenší prvek, tedy A by nebyla DUM.

Důsledek

Každý konečný řetězec je dobře uspořádaný.

Dobře uspořádané množiny

Věta

Mějme dobře uspořádanou množinu A a její podmnožinu B takovou, že existuje izomorfismus $f : A \to B$. Pak pro každý prvek $a \in A$ platí, že $a \leq f(a)$.

Dobře uspořádané množiny

Věta

Mějme dobře uspořádanou množinu A a její podmnožinu B takovou, že existuje izomorfismus $f : A \to B$. Pak pro každý prvek $a \in A$ platí, že $a \leq f(a)$.

Důkaz

Ozn. $K = \{x; x \in A, f(x) < x\}$ a předpokládejme, že $K \neq \emptyset$. Pak K obsahuje nejmenší prvek x_0. Položme $x_1 = f(x_0)$. Protože $x_0 \in K$, je $x_1 = f(x_0) < x_0$. Protože je f izomorfismus, je $f(x_1) < f(x_0) = x_1$, tzn. $x_1 \in K$. Ale to je spor, protože x_0 je nejmenší prvek množiny K. Tedy $K = \emptyset$.

Začátek a jeho vlastnosti

Definice

Nechť A je uspořádaná množina a B její podmnožina. Jestliže pro každé $b \in B$ platí, že $\{x, x \in A, x \leq b\} \subseteq B$, pak se B nazývá začátek množiny A. Pokud je navíc $B \subset A$, nazývá se B vlastní začátek.

Začátek a jeho vlastnosti

Definice

Nechť A je uspořádaná množina a B její podmnožina. Jestliže pro každé $b \in B$ platí, že $\{x, x \in A, x \leq b\} \subseteq B$, pak se B nazývá začátek množiny A. Pokud je navíc $B \subset A$, nazývá se B vlastní začátek.

Věta

Dobře uspořádaná množina není izomorfní s žádným svým vlastním začátkem

Začátek a jeho vlastnosti

Definice

Nechť A je uspořádaná množina a B její podmnožina. Jestliže pro každé $b \in B$ platí, že $\{x, x \in A, x \leq b\} \subseteq B$, pak se B nazývá začátek množiny A. Pokud je navíc $B \subset A$, nazývá se B vlastní začátek.

Věta

Dobře uspořádaná množina není izomorfní s žádným svým vlastním začátkem

Důkaz

A je DUM, B vlastní začátek v A. Pak $B \subset A$, takže $A - B \neq \emptyset$. Množina $A - B$ obsahuje nejmenší prvek a_0. Je zřejmé, že $a_0 > b$ pro všechna $b \in B$. Připusťme, že $\exists X \in B : A \cong X$. Buď $f : A \to X$ izomorfismus. Pak $f(a_0) \in X \subseteq B$, tj. $f(a_0) < a_0$, což dle předchozí věty nelze.

Začátek a jeho vlastnosti

Důsledek

A je DUM, buďte B, C začátky v A. Je-li $B \cong C$, pak $B = C$

Důsledek

A je DUM, buďte B, C začátky v A. Je-li $B \cong C$, pak $B = C$

Důkaz

Je-li $B = A$, $B \cong C$ je $B = C$ dle předchozí věty. Nechť B, C jsou vlastní začátky v A. Je-li $B \neq C$ je B vlastní začátek v C nebo C vlastní začátek v B, pak ale B, C nemohou být podle předchozí věty izomorfní.

Izomorfismy dobře uspořádaných množin

Označme $A(x) = \{t; t \in A, t < x\}$. Uvědomme si, že pro DUM je $A(x)$ vlastní začátek. Navíc pokud je $B \subset A$ vlastní začátek v A, pak existuje $x \in A$ tak, že $B = A(x)$

Izomorfismy dobře uspořádaných množin

Označme $A(x) = \{t; t \in A, t < x\}$. Uvědomme si, že pro DUM je $A(x)$ vlastní začátek. Navíc pokud je $B \subset A$ vlastní začátek v A, pak existuje $x \in A$ tak, že $B = A(x)$

Věta

Buďte A, B dobře uspořádané množiny. Jestliže jsou A, B izomorfní, pak mezi nimi existuje právě jeden izomorfismus.

Izomorfismy dobře uspořádaných množin

Označme $A(x) = \{t; t \in A, t < x\}$. Uvědomme si, že pro DUM je $A(x)$ vlastní začátek. Navíc pokud je $B \subset A$ vlastní začátek v A, pak existuje $x \in A$ tak, že $B = A(x)$

Věta

Buďte A, B dobře uspořádané množiny. Jestliže jsou A, B izomorfní, pak mezi nimi existuje právě jeden izomorfismus.

Důkaz

Buďte $f : A \to B$, $g : A \to B$ izomorfismy a připusťme, že $f \not\equiv g$. Pak $\exists x_0 : f(x_0) \neq g(x_0)$. Protože f je izomorfismus, je $A(x_0) \cong B(f(x_0))$, protože g je izomorfismus, je $A(x_0) \cong B(g(x_0))$. Tzn. $B(f(x_0)) \cong B(g(x_0))$. Podle věty se izomorfní začátky rovnají, tedy $f(x_0) = g(x_0)$, ale to je spor.

Vztah mezi uspořádanými množinami

Věta

Pro dobře uspořádané množiny A, B nastává právě jedna z množností:

- $A \cong B$
- $A \cong B(x)$
- $B \cong A(x)$

pro vhodné $x \in A$, resp. $\in B$.

Úplná indukce

Indukce je výborným prostředkem pro dokazování některých tvrzení platných pro dobře uspořádané množiny:

Úplná indukce

Indukce je výborným prostředkem pro dokazování některých tvrzení platných pro dobře uspořádané množiny:

Úplná indukce

Důkazová metoda o dvou krocích: Nechť $V(n)$ je výroková funkce na přirozených číslech

1. $V(1)$
2. $(\forall n \in \mathbb{N})(V(n) \Longrightarrow V(n+1))$.

Princip transinitní indukce

Transinitní indukce

Nechť A je dobře uspořádaná množina s nejmenším prvkem a_0. Nechť $V(a)$ je výroková funkce na A. Nechť platí:

1. $P(a_0)$ je pravdivý
2. $\forall a \in A$ platí: je-li $P(x)$ pravda $\forall x < a$, je také $P(a)$ pravda.

Pak $P(a)$ je pravda pro všechna $a \in A$.

Princip transinitní indukce

Transinitní indukce

Nechť A je dobře uspořádaná množina s nejmenším prvkem a_0. Nechť $V(a)$ je výroková funkce na A. Nechť platí:

1. $P(a_0)$ je pravdivý
2. $\forall a \in A$ platí: je-li $P(x)$ pravda $\forall x < a$, je také $P(a)$ pravda.

Pak $P(a)$ je pravda pro všechna $a \in A$.

Důkaz

Nechť platí předpoklady. Připusťme, že $A' = \{x; x \in A, P(x) je nepravdivý\} \neq \emptyset$. Protože A je DUM, obsahuje A' nejmenší prvek y_0. Je $y_0 > a_0$, neboť $P(x_0)$ je pravdivý. Pro každé $t \in A, t < y_0$ je výrok pravdivý, takže podle předpokladu je také $P(y_0)$ pravda, což je spor. Tedy $A' = \emptyset$.

Axiom výběru

Příklad

Na $\mathbb{R}$ definujeme relaci $\varrho = \{[x, y], x, y \in \mathbb{R}, x - y \in \mathbb{Q}\}$ Kdybychom $\mathbb{R}$ "rozkouskovali" podle této relace, tak dostaneme opět nekonečnou množinu a nevíme jakým způsobem vybrat z každé takové skupinky jeden prvek. To, že to možné (přestože nevíme jak) zaručuje axiom výběru.

Příklad

Na $\mathbb{R}$ definujeme relaci $\varrho = \{[x, y], x, y \in \mathbb{R}, x - y \in \mathbb{Q}\}$ Kdybychom $\mathbb{R}$ "rozkouskovali" podle této relace, tak dostaneme opět nekonečnou množinu a nevíme jakým způsobem vybrat z každé takové skupinky jeden prvek. To, že to možné (přestože nevíme jak) zaručuje axiom výběru.

Axiom výběru

Nechť A je libovolná neprázdná množina, nechť M_a je neprázdná množina pro každé $a \in A$ a navíc M_a jsou po dvou disjunktní. Pak existuje množina M tak, že:

1. $M \subseteq \bigcup_{a \in A} M_a$
2. $M \cap M_a$ je jednoprvková pro každé $a \in A$

Věty ekvivalentní s axiomem výběru

- Zermelova věta: Na každé množině existuje dobré uspořádání
- Hausdorfova věta: Každý řetězec uspořádané množiny je podmnožinou některého maximálního řetězce této množiny
- Zornovo lemma: Je-li každý řetězec uspořádané množiny A shora ohraničený, existuje ke každému prvku $a \in A$ maximální prvek $a_m \in A$ tak, že $a \leq a_m$

Ekvivalentní a spočetné množiny

Definice

Řekneme, že množiny A, B jsou ekvivalentní, jestliže existuje bijektivní zobrazení $f : A \to B$, ozn. $A \sim B$

Ekvivalentní a spočetné množiny

Definice

Řekneme, že množiny A, B jsou ekvivalentní, jestliže existuje bijektivní zobrazení $f : A \to B$, ozn. $A \sim B$

Definice

Množina A je spočetná, jestliže je ekvivalentní s množinou přirozených čísel. Množina, která je konečná nebo spočetná se nazývá nejvýše spočetná

Ekvivalentní a spočetné množiny

Definice

Řekneme, že množiny A, B jsou ekvivalentní, jestliže existuje bijektivní zobrazení $f : A \to B$, ozn. $A \sim B$

Definice

Množina A je spočetná, jestliže je ekvivalentní s množinou přirozených čísel. Množina, která je konečná nebo spočetná se nazývá nejvýše spočetná

- Prvky spočetných množin lze tedy uspořádat do posloupnosti
- Podmnožina spočetná množiny je nejvýše spočetná

Spočetné množiny

Věta

Nechť I je nejvýše spočetná a nechť A_i je rovněž nejvýše spočetná pro každé $i \in I$. Pak $\bigcup_{i \in I} A_i$ také spočetná.

Spočetné množiny

Věta

Nechť I je nejvýše spočetná a nechť A_i je rovněž nejvýše spočetná pro každé $i \in I$. Pak $\bigcup_{i \in I} A_i$ také spočetná.

Důkaz

Každou z množin A_i můžeme uspořádat do posloupnosti

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13}, \dots\} \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \dots\} \\ A_3 &= \{a_{31}, a_{32}, a_{33}, \dots\} \\ &\vdots \end{aligned}$$

Pak ale $\bigcup_{i \in I} = \{a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots\}$

Důsledek

Množina celých čísel je spočetná

Spočetné množiny

Důsledek

Množina celých čísel je spočetná

Věta

Každá nekonečná množina A obsahuje spočetnou množinu B takovou, že množina $A - B$ je nekonečná.

Spočetné množiny

Důsledek

Množina celých čísel je spočetná

Věta

Každá nekonečná množina A obsahuje spočetnou množinu B takovou, že množina $A - B$ je nekonečná.

Důkaz

Je-li A nekonečná, existují $a_1, b_1 \in A$, $a_1 \neq b_1$. Protože $A - \{a_1, b_1\}$ je také nekonečná, existují $a_2, b_2 \in A - \{a_1, b_1\}$, $a_2 \neq b_2, \ldots$ Indukcí takto sestrojíme dvě podmožiny $B = (a_n)_{n=1}^{\infty}$, $C = (b_n)_{n=1}^{\infty}$

Spočetné množiny

Věta

Kartézský součin dvou spočetných množin je spočetná množina.

Spočetné množiny

Věta

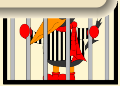
Kartézský součin dvou spočetných množin je spočetná množina.

Důkaz

Jistě platí, že $A \sim C, B \sim D \Rightarrow A \times B \sim C \times D$. Stačí tedy ukázat, že $\mathbb{N} \times \mathbb{N}$ je spočetná. Pro každý prvek $(p, q) \in \mathbb{N} \times \mathbb{N}$ označíme výškou toho prvku číslo $p + q$. Pro $\forall n \in \mathbb{N}$ tedy dostáváme $n - 1$ dvojic výšky n. Označme P_n množinu všech dvojic výšky n. Pak

$$\mathbb{N} \times \mathbb{N} = \bigcup_{n=2}^{\infty}$$

a ta je podle věty spočetná



Spočetné množiny

Věta

Kartézský součin dvou spočetných množin je spočetná množina.

Důkaz

Jistě platí, že $A \sim C, B \sim D \Rightarrow A \times B \sim C \times D$. Stačí tedy ukázat, že $\mathbb{N} \times \mathbb{N}$ je spočetná. Pro každý prvek $(p, q) \in \mathbb{N} \times \mathbb{N}$ označíme výškou toho prvku číslo $p + q$. Pro $\forall n \in \mathbb{N}$ tedy dostáváme $n - 1$ dvojic výšky n. Označme P_n množinu všech dvojic výšky n. Pak

$$\mathbb{N} \times \mathbb{N} = \bigcup_{n=2}^{\infty}$$

a ta je podle věty spočetná

Důsledek

Množina racionálních čísel je spočetná

Spočetné množiny

Věta

Množina konečných posloupností prvků spočetné množiny je spočetná

Spočetné množiny

Věta

Množina konečných posloupností prvků spočetné množiny je spočetná

Důkaz

Nechť $n \in \mathbb{N}$ je libovolná. Podle věty je A^n (množina všech uspořádaných n-tic) spočetná. Tedy

$$K = \bigcup_{n=1}^{\infty} A^n$$

je podle věty o sjednocení spočetných množin také spočetná

Spočetné množiny

Věta

Množina konečných posloupností prvků spočetné množiny je spočetná

Důkaz

Nechť $n \in \mathbb{N}$ je libovolná. Podle věty je A^n (množina všech uspořádaných n-tic) spočetná. Tedy

$$K = \bigcup_{n=1}^{\infty} A^n$$

je podle věty o sjednocení spočetných množin také spočetná

Důsledek

Množina všech polynomů jedné proměnné s racionální koeficienty je spočetná

Kardinální čísla

Definice

Každé množině A přiřadíme symbol *card* A a budeme mu říkat kardinální číslo (někdy také mohutnost) tak, aby byla splněna následující podmínka:

$$\mathit{card}\ A = \mathit{card}\ B \Leftrightarrow A \sim B$$

Kardinální čísla

Definice

Každé množině A přiřadíme symbol $card\ A$ a budeme mu říkat kardinální číslo (někdy také mohutnost) tak, aby byla splněna následující podmínka:

$$card\ A = card\ B \Leftrightarrow A \sim B$$

Pro konečnou množinu A o n prvcích je $card\ A = n$, $card\ \mathbb{N} = \aleph_0$ (čteme "alef")

Kardinální čísla

Definice

Každé množině A přiřadíme symbol *card* A a budeme mu říkat kardinální číslo (někdy také mohutnost) tak, aby byla splněna následující podmínka:

$$card\ A = card\ B \Leftrightarrow A \sim B$$

Pro konečnou množinu A o n prvcích je $card\ A = n$, $card\ \mathbb{N} = \aleph_0$ (čteme "alef")

Porovnávání kardinálních čísel

$card\ A \leq card\ B \iff$ existuje injektivní zobrazení $f : A \to B$

Kardinální čísla

Definice

Každé množině A přiřadíme symbol *card* A a budeme mu říkat kardinální číslo (někdy také mohutnost) tak, aby byla splněna následující podmínka:

$$card\ A = card\ B \Leftrightarrow A \sim B$$

Pro konečnou množinu A o n prvcích je $card\ A = n$, $card\ \mathbb{N} = \aleph_0$ (čteme "alef")

Porovnávání kardinálních čísel

$card\ A \leq card\ B \Longleftrightarrow$ existuje injektivní zobrazení $f : A \to B$

POZOR! Všechny kardinální čísla netvoří množinu, ale třídu. Ukážeme si to později.

Kardinální čísla

Cantor-Bernsteinova věta

Buďte A, B libovolné množiny. Existují-li $A_1 \subseteq A$, $B_1 \subseteq B$ tak, že $A \sim B_1$ a současně $B \sim A_1$, pak platí, že $A \sim B$

Kardinální čísla

Cantor-Bernsteinova věta

Buďte A, B libovolné množiny. Existují-li $A_1 \subseteq A$, $B_1 \subseteq B$ tak, že $A \sim B_1$ a současně $B \sim A_1$, pak platí, že $A \sim B$

Věta

Každá množina kardinálních čísel je uspořádaná, dokonce platí, že každá dvě kardinální čísla jsou porovnatelná

Kardinální čísla

Cantor-Bernsteinova věta

Buďte A, B libovolné množiny. Existují-li $A_1 \subseteq A$, $B_1 \subseteq B$ tak, že $A \sim B_1$ a současně $B \sim A_1$, pak platí, že $A \sim B$

Věta

Každá množina kardinálních čísel je uspořádaná, dokonce platí, že každá dvě kardinální čísla jsou porovnatelná

Důkaz

Ověříme zda je relace $\leq$ uspořádání, tj. zda je reflexivní, antisymetrická a tranzitivní.

Kardinální čísla

Věta

Každá dvě kardinální čísla jsou srovnatelná, tj. $a \leq b$ nebo $b \leq a$

Kardinální čísla

Věta

Každá dvě kardinální čísla jsou srovnatelná, tj. $a \leq b$ nebo $b \leq a$

Důkaz

Nechť $a = card\ A$, $b = card\ B$. Podle Zermelovy věty existuje na A, B dobré uspořádání, tedy pro ně musí platit jeden ze vztahů mezi DUM.

Kardinální čísla

Věta

Každá dvě kardinální čísla jsou srovnatelná, tj. $a \leq b$ nebo $b \leq a$

Důkaz

Nechť $a = card\ A$, $b = card\ B$. Podle Zermelovy věty existuje na A, B dobré uspořádání, tedy pro ně musí platit jeden ze vztahů mezi DUM.

Cantorova věta

Nechť A, B jsou neprázdné množiny a $card\ A \geq 2$. Pak $card\ A^B > card\ B$

Kardinální čísla

Věta

Každá dvě kardinální čísla jsou srovnatelná, tj. $a \leq b$ nebo $b \leq a$

Důkaz

Nechť $a = card\ A$, $b = card\ B$. Podle Zermelovy věty existuje na A, B dobré uspořádání, tedy pro ně musí platit jeden ze vztahů mezi DUM.

Cantorova věta

Nechť A, B jsou neprázdné množiny a $card\ A \geq 2$. Pak $card\ A^B > card\ B$

Důsledek

Existují nespočetné množiny. Dokonce platí, že kardinálních čísel větších než $\aleph_0$ je nekonečně mnoho

Nespočetnost reálných čísel a intervalu (0,1)

Věta

$(0, 1)$ je nespočetná množina

Nespočetnost reálných čísel a intervalu (0,1)

Věta

$(0,1)$ je nespočetná množina

Důsledek

Množina $\mathbb{R}$ je nespočetná a navíc $\mathbb{R} \sim (0,1)$

Nespočetnost reálných čísel a intervalu (0,1)

Věta

$(0,1)$ je nespočetná množina

Důsledek

Množina $\mathbb{R}$ je nespočetná a navíc $\mathbb{R} \sim (0,1)$

Důkaz

Zobrazení $f(x) = \operatorname{arctg}\ x$ je bijekce $\mathbb{R}$ na interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Navíc platí, že každé dva intervaly $(a_1, b_1), (a_2, b_2)$ jsou ekvivalentní neboť $f(x) = \frac{b_2 - b_1}{a_2 - a_1}(x - a_1) + b_1$. Tedy $(0,1) \sim \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \sim \mathbb{R}$

Nespočetnost reálných čísel a intervalu (0,1)

Věta

$(0, 1)$ je nespočetná množina

Důsledek

Množina $\mathbb{R}$ je nespočetná a navíc $\mathbb{R} \sim (0, 1)$

Důkaz

Zobrazení $f(x) = \operatorname{arctg}\, x$ je bijekce $\mathbb{R}$ na interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Navíc platí, že každé dva intervaly $(a_1, b_1), (a_2, b_2)$ jsou ekvivalentní neboť $f(x) = \frac{b_2 - b_1}{a_2 - a_1}(x - a_1) + b_1$. Tedy $(0, 1) \sim \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \sim \mathbb{R}$

Důsledek

Iracionální čísla jsou nespočetná množina.

Počítání s kardinálními čísly

Věta

Buď A libovolná množina. Pak $card\ \mathcal{P}(A) > card\ A$

Počítání s kardinálními čísly

Věta

Buď A libovolná množina. Pak $card\ \mathcal{P}(A) > card\ A$

Důkaz

Je-li $A = \emptyset$, pak $card\ A = 0, card\ \mathcal{P}(A) = 1$. Nechť $A \neq \emptyset$. Zvolme $B = \{0, 1\}$. Definujme zobrazení $F : B^A \to \mathcal{P}(A)$ takto:

$$\forall f : A \to B \text{ je } F(f) = \{x, x \in A, f(x) = 0\}$$

Pak zřejmě F je bijekce a tvrzení plyne z Cantorovy věty, tj.

$$card\ \mathcal{P}(A) = card\ B^A > card\ A$$

Věta

Buď A libovolná nespočetná, $B \subseteq A$ nejvýše spočetná. Pak $card\ A = card\ (A - B)$

Počítání s kardinálními čísly

Věta

Buď A libovolná nespočetná, $B \subseteq A$ nejvýše spočetná. Pak $card\ A = card\ (A - B)$

Důkaz

Je $A = (A - B) \cup A$. Protože B je nejvýše spočetná, je $A - B$ nekonečná. POdle věty existuje spočetná množina $A_1 \subseteq A - B$. Ozn. $P = (A - B) - A_1$. Pak je $A - B = A_1 \cup P$, tj. $A = (B \cup A_1) \cup P$. Protože je možina $B \cup A_1$ spočetná, existuje bijekce $f : A_1 \to B \cup A_1$. Položme pro každé $x \in A - B$:

- $g(x) = f(x)$ pro $x \in A_1$
- $g(x) = x$ pro $x \in P$

Pak $g : (A - B) \to A$ je bijekce

Počítání s kardinálními čísly

Důsledek

Buď A libovolná nekonečná, B nejvýše spočetná. Pak
$card\ A = card\ (A \cup B)$

Počítání s kardinálními čísly

Důsledek

Buď A libovolná nekonečná, B nejvýše spočetná. Pak $\mathit{card}\ A = \mathit{card}\ (A \cup B)$

Věta

Množina je nekonečná, je-li ekvivalentní s některou svou vlastní podmnožinou.

Počítání s kardinálními čísly

Důsledek

Buď A libovolná nekonečná, B nejvýše spočetná. Pak
$card\ A = card\ (A \cup B)$

Věta

Množina je nekonečná, je-li ekvivalentní s některou svou vlastní podmnožinou.

Konečná kardinální čísla můžeme sčítat, násobit a umocňovat - tyto operace odpovídají operacím sjednocení, průniku a kartézské mocnině

Mohutnost kontinua

- Mohutností kontinua nazýváme kardinální číslo $2^{\aleph_0}$, ozn. $\mathbf{c}$
- Počítáme s $\mathbf{c}$:
  - $n + \mathbf{c} = \aleph_0 + \mathbf{c} = \mathbf{c} + \mathbf{c} = \mathbf{c}$
  - $n \cdot \mathbf{c} = \aleph_0 \cdot \mathbf{c} = \mathbf{c} \cdot \mathbf{c} = \mathbf{c}$
  - $\mathbf{c}^n = \mathbf{c}$
  - $n > 1 : n^{\aleph_0} = \aleph_0^{\aleph_0} = \mathbf{c}^{\aleph_0} = \mathbf{c}$
- Množiny s mohutností kontinua:
  - $\mathbb{R}$
  - $\mathbb{R}^n$
  - libovolný interval reálných čísel
  - iracionální čísla
  - množina posloupností přirozených čísel
  - množina všech podmnožin $\mathbb{N}$
- Hypotéza kontinua: Neexistuje kardinální číslo k takové, že $\aleph_0 < k < \mathbf{c}$

Ordinální typy a čísla

Definice

Uspořádané množiny A, B mají stejný ordinální typ, jestliže $A \cong B$, píšeme $\overline{A} = \overline{B}$.

Ordinální typy a čísla

Definice

Uspořádané množiny A, B mají stejný ordinální typ, jestliže $A \cong B$, píšeme $\overline{A} = \overline{B}$.

Ordinální typ konečného řetězce o n prvcích označujeme n, $\overline{\mathbb{N}} = \omega$

Ordinální typy a čísla

Definice

Uspořádané množiny A, B mají stejný ordinální typ, jestliže $A \cong B$, píšeme $\overline{A} = \overline{B}$.

Ordinální typ konečného řetězce o n prvcích označujeme n, $\overline{\mathbb{N}} = \omega$

Ordinální typy můžeme opět sčítat, násobit, umocňovat. Tomu odpovídají operace součet, součin a mocnina uspořádaných množin.

Ordinální typy a čísla

Definice

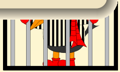
Uspořádané množiny A, B mají stejný ordinální typ, jestliže $A \cong B$, píšeme $\overline{A} = \overline{B}$.

Ordinální typ konečného řetězce o n prvcích označujeme n, $\overline{\mathbb{N}} = \omega$

Ordinální typy můžeme opět sčítat, násobit, umocňovat. Tomu odpovídají operace součet, součin a mocnina uspořádaných množin.

Definice

Ordinální typ dobře uspořádané množiny nazýváme ordinální číslo



Ordinální čísla

Definice

Mějme ordinální čísla α, β příslušející množinám A, B. Řekneme, že $\alpha \leq \beta$ jestliže A je izomorfní s nějakým začátkem množiny B.

Ordinální čísla

Definice

Mějme ordinální čísla α, β příslušející množinám *A*, *B*. Řekneme, že $\alpha \leq \beta$ jestliže *A* je izomorfní s nějakým začátkem množiny *B*.

Každá dvě ordinální čísla jsou porovnatelná

Ordinální čísla

Definice

Mějme ordinální čísla α, β příslušející množinám A, B. Řekneme, že $\alpha \leq \beta$ jestliže A je izomorfní s nějakým začátkem množiny B.

Každá dvě ordinální čísla jsou porovnatelná

Důkaz

Plyne ze vztahu mezi DUM.

Ordinální čísla

Definice

Symbolem $W(\alpha)$ označujeme množinu všech ordinálních čísel ostře menších než α

Ordinální čísla

Definice

Symbolem $W(\alpha)$ označujeme množinu všech ordinálních čísel ostře menších než α

Věta

$\overline{W(\alpha)} = \alpha$

Ordinální čísla

Definice

Symbolem $W(\alpha)$ označujeme množinu všech ordinálních čísel ostře menších než α

Věta

$\overline{\overline{W(\alpha)}} = \alpha$

Důkaz

Nechť α je ordinální číslo množiny A. Pro každé $x \in A$ označme $\varphi(x)$ ordinální typ $A(x)$. Pak zřejmě φ je zobrazení A do $W(\alpha)$. Ukážeme, že je to izomorfismus. Nechť $\beta \in W(\alpha)$ libovolné. Pak $\beta < \alpha$. Pak ke každé množině B takové, že $\overline{\overline{B}} = \beta$, existuje $x \in A$ tak, že $B \cong A(x)$, tj. $\beta = \varphi(x)$. Tedy φ je surjekce. Pro $x, y \in A, x < y$ je zřejmě $\overline{\overline{A(x)}} < \overline{\overline{A(y)}}$, tj. $\varphi(x) < \varphi(y)$. Tedy φ je izotonní injekce. Je zřejmě $\varphi^{-1} : W(\alpha) \to A$ také izotonní, tedy φ je izomorfismus.

Ordinální čísla

Věta

Každá množina ordinálních čísel je dobře uspořádaná

Ordinální čísla

Věta

Každá množina ordinálních čísel je dobře uspořádaná

Věta

Každé ordinální číslo má svého bezprostředního následníka

Ordinální čísla

Věta

Každá množina ordinálních čísel je dobře uspořádaná

Věta

Každé ordinální číslo má svého bezprostředního následníka

Definice

Buď m nekonečné kardinální číslo. Symbolem $Z(m)$ označujeme množinu všech ordinálních čísel mohutnosti m. Nejmenší z nich se nazývá počáteční ordinální číslo a značí se $\omega(m)$

Ordinální čísla

Věta

Každá množina ordinálních čísel je dobře uspořádaná

Věta

Každé ordinální číslo má svého bezprostředního následníka

Definice

Buď m nekonečné kardinální číslo. Symbolem $Z(m)$ označujeme množinu všech ordinálních čísel mohutnosti m. Nejmenší z nich se nazývá počáteční ordinální číslo a značí se $\omega(m)$

Označení

Buď m nekonečné kardinální číslo.

$$\mathcal{A}(m) := \{\omega(n); \aleph_0 \leq n < m\}$$

Ordinální čísla

Definice

Nechť m je nekonečné kardinální číslo a nechť $\overline{\mathcal{A}(m)} = \alpha$. Pak $\omega(m)$ označujeme ω_α a m označujeme $\aleph_\alpha$

Ordinální čísla

Definice

Nechť m je nekonečné kardinální číslo a nechť $\overline{\mathcal{A}(m)} = \alpha$. Pak $\omega(m)$ označujeme ω_α a m označujeme $\aleph_\alpha$

Věta

Každé nekonečné číslo je některým alefem.

Ordinální čísla

Definice

Nechť m je nekonečné kardinální číslo a nechť $\overline{\mathcal{A}(m)} = \alpha$. Pak $\omega(m)$ označujeme ω_α a m označujeme $\aleph_\alpha$

Věta

Každé nekonečné číslo je některým alefem.

Věta

Každé ordinální číslo je indexem některého alefu

Ordinální čísla

Definice

Nechť *m* je nekonečné kardinální číslo a nechť $\overline{\mathcal{A}(m)} = \alpha$. Pak $\omega(m)$ označujeme ω_α a *m* označujeme $\aleph_\alpha$

Věta

Každé nekonečné číslo je některým alefem.

Věta

Každé ordinální číslo je indexem některého alefu

Počítání s alefy

- $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_{\max(\alpha,\beta)}$
- $card\ Z(\aleph_\alpha) = \aleph_{\alpha+1}$