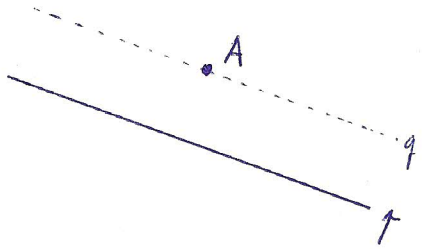
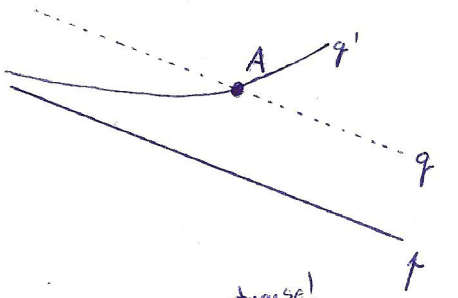
Axiomatická výstavba matematických teorií

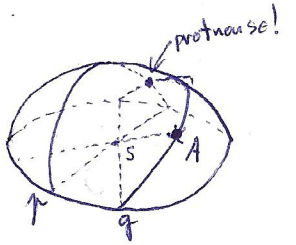
Problém: Je dán bod A a přímka p tak, že $A \notin p$. Kolik přímek můžeme vést bodem A tak, aby neprotly přímku p?



JEDINOU! (Řešení pana Euklida cca 300 př.n.l.)



KLIDNĚ NEKONEČNĚ MNOHO (Šokující řešení pana Lobačevského cca 13.2. 1826)



TŘEBA ŽÁDNOU (eliptická geometrie)

⇒ Záleží na tom, jak si představujeme přímku! ⇒

Základní (primitivní) pojmy: Pojmy z nichž při budování teorie vycházíme. Nedefinujeme je. Např. bod, přímka, ... (při budování teorie geometrie)

Soustava axiomů: V axiomech jsou popsány vztahy mezi základními pojmy. Tím vymezujeme naše představy o základních pojmech

Např.: 1) $\forall A,B \in \mathcal{B}\ \exists! p \in \mathcal{P} : (A \in p \wedge B \in p)$

2) $\forall p \in \mathcal{P}\ \forall A \in \mathcal{B},\ A \notin p\ \exists! q \in \mathcal{P} : (A \in q \wedge p \parallel q)$

⋮

Definice: na základě základních pojmů a dříve definovaných pojmů tvoříme v definicích pojmy nové. např. Kolmice je přímka, která ....

Věty: Pomocí matematické logiky odvozujeme ze soustavy axiomů a dříve dokázaných vět ~~dokazujeme~~ další věty (pravdivé výroky).

Výroky a logické spojky

Výrok ... je to věta jíž je možno přiřadit jednu ze dvou pravdivostních hodnot: pravda (0), nepravda (1)

Př.: „Auto je modré." je výrok; „Otevři okno!" není výrok

Negace výroku: Negací výroku A je výrok „Není pravda, že A." Značíme: non A; $\neg A$; A'. Pravdivostní tabulka:

A	A'
1	0
0	1

.

Konjunkce výroků: Tvoříme ji pomocí logické spojky „a zároveň" ($\wedge$).

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

Konjunkce výroků A a B je pravdivá pouze pokud jsou oba výroky pravdivé.

Disjunkce výroků: Tvoříme ji pomocí logické spojky „nebo" ($\vee$).

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

Disjunkce výroků A a B je pravdivá pokud je pravdivý alespoň jeden z výroků A, B.

Implikace výroků: Tvoříme ji pomocí logické spojky „jestliže - pak" ($\Rightarrow$).

A	B	$A \Rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Implikace výroků A a B je nepravdivá pouze v případě, že A je pravda a B je nepravda.

Ekvivalence výroků: Tvoříme ji pomocí logické spojky „právě tehdy když." ($\Leftrightarrow$)

A	B	$A \Leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

$A \Leftrightarrow B$ je logicky ekvivalentní s $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

VÝROK	JEHO NEGACE
A'	A
$A \wedge B$	$A' \vee B'$
$A \vee B$	$A' \wedge B'$
$A \Rightarrow B$	$A \wedge B'$
$A \Leftrightarrow B$	$(A \wedge B') \vee (B \wedge A')$

Dokažte, že $[(A \Rightarrow A_1) \wedge (A_1 \Rightarrow A_2)] \Rightarrow (A \Rightarrow A_2)$ je tautologie.

(Princip přímého důkazu.)

Dokazovanou výrokovou formuli označme X. Potom:

A	A_1	A_2	$A \Rightarrow A_1$	$A_1 \Rightarrow A_2$	$(A \Rightarrow A_1) \wedge (A_1 \Rightarrow A_2)$	$A \Rightarrow A_2$	X
1	1	1	(1)	(1)	1	(1)	1
0	1	1	(1)	(1)	1	(1)	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
1	0	0	0	1	0	0	1
0	0	0	(1)	(1)	1	(1)	1

Z tabulky je vidět, že v případě, že $A \Rightarrow A_1$ je pravda a také $A_1 \Rightarrow A_2$ je pravda, pak je pravdivý i výrok $A \Rightarrow A_2$. Tato je základem tzv. přímého důkazu.

Kvantifikované výroky

Kvantifikátory: $\forall$ ... pro každé

$\exists$ ... existuje

$\exists!$ ... existuje právě jeden (jedno)

Výroková forma: je to věta obsahující jednu, nebo více proměnných.

Například: a) Auto x je modré.

b) Pro reálná čísla x a y platí, že $x < y$.

Kvantifikovaný výrok: Vznikne spojením kvantifikátoru a výrokové formy.

Například:

„Pro každé reálné číslo x platí, že $x^2 \geq 0$."

$\forall x \in \mathbb{R} \quad : \quad x^2 \geq 0$

Výrok	Negace
$\forall x \in A : V(x)$	$\exists x \in A : \text{non } V(x)$
$\exists x \in A : V(x)$	$\forall x \in A : \text{non } V(x)$
$\exists! x \in A : V(x)$	$(\forall x \in A : \text{non } V(x)) \vee (\exists x \in A \, \exists y \in A : x \neq y \wedge V(x) \wedge V(y))$
$\forall x \in M \, \forall y \in Z : V(x,y)$	$\exists x \in M \, \exists y \in Z : \text{non } V(x,y)$
$\forall x \in M \, \exists y \in Z : V(x,y)$	$\exists x \in M \, \forall y \in Z : \text{non } V(x,y)$
$\exists x \in M \, \forall y \in Z : V(x,y)$	$\forall x \in M \, \exists y \in Z : \text{non } V(x,y)$
$\exists x \in M \, \exists y \in Z : V(x,y)$	$\forall x \in M \, \forall y \in Z : \text{non } V(x,y)$
$\exists y \in Z \, \exists x \in M : V(x,y)$	
$\forall y \in Z \, \forall x \in M : V(x,y)$	
$\exists y \in Z \, \forall x \in M : V(x,y)$	

totéž — totéž — totéž — totéž — není totéž

Typy důkazů

Pokud není pravdivost matematické věty na první pohled zřejmá, je třeba provést důkaz její pravdivosti. Existuje několik základních způsobů jak to provést.

Přímý důkaz: Je možné použít pro důkaz pravdivosti výroku: $\boxed{A \Rightarrow B}$

Snažíme se najít výroky $A_1, A_2, \dots, A_n$ tak, aby byla zřejmá pravdivost implikací:

$$A \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \dots \Rightarrow A_n \Rightarrow B$$

Pokud se nám to podaří, je jistě pravdivý i výrok $A \Rightarrow B$.

Př.: 1) **Věta:** Nechť $\underbrace{a \text{ je sudé číslo}}_{A}$, pak $\Rightarrow$ $\underbrace{a^2 \text{ je také sudé číslo}}_{B}$.

Důkaz (přímý):

$$\underbrace{a \text{ je sudé číslo}}_{A} \Rightarrow \underbrace{a = 2k, \text{ kde } k \in \mathbb{Z}}_{A_1} \Rightarrow \underbrace{a^2 = 4k^2}_{A_2} \Rightarrow \underbrace{a^2 = 2 \cdot (2k^2)}_{A_3} \Rightarrow$$

$$\Rightarrow \underbrace{a^2 \text{ je sudé číslo}}_{B} \quad \square$$

někdy to není tak pěkně vidět, přesto jde o důkaz přímý (ve své podstatě)

2.) **Věta:** Nechť $A \Rightarrow B$ je výrok. Potom výrok $B' \Rightarrow A'$ má stejnou pravdivostní hodnotu.

Důkaz:

A	B	B'	A'	A⇒B	B'⇒A'
1	1	0	0	1	1
1	0	1	0	0	0
0	1	0	1	1	1
0	0	1	1	1	1

$\square$

Nepřímý důkaz: Dokazujeme-li pravdivost výroku $A \Rightarrow B$, můžeme využít toho, že výrok $B' \Rightarrow A'$ má jistě stejnou pravdivostní hodnotu. Podaří-li se dokázat $B' \Rightarrow A'$ (věta obměněná) je jistě pravdivá i dokazovaná věta $A \Rightarrow B$.

Př.: *Dokažte, že pro každé přirozené číslo n platí: Jestliže je n^2 sudé, pak n je také sudé.*

Budeme tedy dokazovat větu, jíž jsme využili v důkazu v Příkladu 7. Tentokrát jsme ji formulovali slovy, můžeme však přidat také symbolický zápis, jaký najdeme ve většině ostatních příkladů: $\forall(n \in \mathbb{N})$: $2|n^2 \Rightarrow 2|n$.

K důkazu opět použijeme obměněnou implikaci, budeme tedy dokazovat větu: $\forall(n \in \mathbb{N})$: $2\nmid n \Rightarrow 2\nmid n^2$

Je-li n liché (tedy nedělitelné dvěma), pak je možné psát $n = 2k + 1$, kde k je nějaké přirozené číslo nebo nula. Zkusíme-li toto číslo umocnit na druhou, získáme:

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Označíme-li přirozené číslo $(2k^2 + 2k)$ jako r, zjistíme, že číslo $(2k + 1)^2$ je rovno číslu $(2r + 1)$, které jistě dělitelné dvěma. Tím jsme dokázali obměněnou a tedy i původní implikaci.

Př.:

Dokažte: $\forall(n \in \mathbb{N})$: $5|(n^2 + 1) \Rightarrow 5|n$.

Nejprve zkonstruujeme obměněnou implikaci (kvantifikátor se nemění): $\forall(n \in \mathbb{N})$: $5|n \Rightarrow 5\nmid(n^2 + 1)$. Tuto větu budeme nyní dokazovat (přímým důkazem). Musíme tedy vyjít z předpokladu, že n je dělitelné pěti. Můžeme tedy psát $n = 5k$, kde k je nějaké přirozené číslo. Nyní dosaďme $(5k)$ za n do výrazu $(n^2 + 1)$ a pokusme se prokázat, že tak získáme číslo, které není dělitelné pěti:

$$n^2 + 1 = (5k)^2 + 1 = 25k^2 + 1 = 5(5k^2) + 1$$

Můžeme říci, že existuje přirozené číslo r takové, že $5k^2 = r$. Pak lze psát $n^2 + 1 = 5r + 1$. Je zřejmé, že číslo $(5r + 1)$ není dělitelné pěti, tedy i číslo $(n^2 + 1)$ není dělitelné pěti. Tím jsme dokázali obměněnou implikaci a díky ní i původní větu.

Důkaz sporem: Dokazujeme, že platí výrok A. Stačí dokázat, že A' není pravda. (Pokud dokazujeme větu ve tvaru $A \Rightarrow B$, ukážeme, že nemůže nastat její negace, to jest $A \wedge B'$).)

Př: **Věta:** Existuje nekonečně mnoho prvočísel.

Důkaz: A: Existuje nekonečně mnoho prvočísel.

Vyjdeme z: A': Existuje konečně mnoho prvočísel

$\Downarrow$

A_1: Existují pouze prvočísla $p_1, p_2, \dots, p_k$

označme $n = p_1 p_2 \dots p_k + 1$

(víme, že každé přirozené číslo je dělitelné součinem prvočísel)

$\Downarrow$

A_2: Některé z prvočísel - označme jej p_i dělí číslo n, tzn

$n = p_i \cdot k$, kde $k \in \mathbb{Z}$

$\Downarrow$

A_3:

$$p_i \cdot k = n = p_1 p_2 \dots p_k + 1 \quad / : p_i$$

$$k = \underbrace{\frac{p_1 p_2 \dots \cancel{p_i} \dots p_k}{\cancel{p_i}}}_{\in \mathbb{Z}} + \underbrace{\frac{1}{p_i}}_{\in (0,1)}$$

$\Downarrow$

A_4: $k \notin \mathbb{Z}$ - ale to není pravda !!! Spor! □

Tzn: Dokázali jsme, že platí: $A' \Rightarrow A_4$ (To je pravdivý výrok)

Ale víme, že A_4 není pravda - tato kombinace se vyskytuje pouze ve čtvrtém řádku násl. pravdivostní tabulky

A'	A_4	$A' \Rightarrow A_4$
1	1	1
1	0	0
0	1	1
0	0	1

$A' \Rightarrow A_4$ je pravda

A_4 není pravda

$\Rightarrow$ pouze v případě $p(A') = 0$

$\Rightarrow$ je jediná možnost, a to, že A je pravda! □

Důkaz slabou matematickou indukcí:

Použití: Matematickou indukcí dokazujeme věty typu

$$\forall n \in \mathbb{N} : V(n)$$

Postup: 1.) Dokážeme pravdivost $V(1)$.

2.) Dokážeme pravdivost implikace $V(n) \Rightarrow V(n+1)$. (pro každé $n \in \mathbb{N}$)

Příklad:

Př.1: Dokažte, že $\forall n \in \mathbb{N} : 1+q+q^2+\ldots+q^{n-1} = \frac{q^n-1}{q-1}$ pro $q \neq 1$.

1.) $n=1 \Rightarrow L=1$; $P = \frac{q^1-1}{q-1} = 1 \Rightarrow L=P \Rightarrow$ pravda

2.) Předpokládejme, že platí $V(n)$: $1+q+q^2+\ldots+q^{n-1} = \frac{q^n-1}{q-1}$

(Máme dokázat, že potom také platí $V(n+1)$: $1+q+q^2+\ldots+q^n = \frac{q^{n+1}-1}{q-1}$)

$$\Rightarrow 1+q+q^2+\ldots+q^n = \underbrace{1+q+q^2+\ldots+q^{n-1}}_{\text{předpoklad} \Rightarrow} + q^n = \frac{q^n-1}{q-1} + q^n =$$

$$= \frac{q^n-1+q^n(q-1)}{q-1} = \frac{q^n-1+q^{n+1}-q^n}{q-1} = \frac{q^{n+1}-1}{q-1}$$

□

Př.2: Dokažte, že $\forall n \in \mathbb{N} : 1+2+3+\ldots+n = \frac{n(n+1)}{2}$

1.) $n=1 \Rightarrow L=1$; $P = \frac{1\cdot(1+1)}{2} = 1 \Rightarrow L=P \Rightarrow$ pravda

2.) Předpoklad: $1+2+3+\ldots+n = \frac{n(n+1)}{2}$.

(Máme dokázat: $1+2+3+\ldots+(n+1) = \frac{(n+1)(n+2)}{2}$)

$$1+2+3+\ldots+(n+1) = \underbrace{1+2+3+\ldots+n}_{} + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+(n+1)\cdot 2}{2} = \frac{(n+1)(n+2)}{2}$$

□

Př3: Dokažte, že $\forall n \in \mathbb{N}: 1^2+2^2+3^2+\dots+n^2 = \frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$

1.) $n=1 \Rightarrow L=1$, $P = \frac{1}{3}+\frac{1}{2}+\frac{1}{6} = \frac{2+3+1}{6} = 1 \Rightarrow$ pravda

2.) Předpoklad: $1^2+2^2+3^2+\dots+n^2 = \frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$

(Máme dokázat: $\underbrace{1^2+2^2+3^2+\dots+(n+1)^2}_{L} = \underbrace{\frac{1}{3}(n+1)^3+\frac{1}{2}(n+1)^2+\frac{1}{6}(n+1)}_{P}$)

1
1 2 1
1 3 3 1

$$P = \frac{1}{3}(n^3+3n^2+3n+1)+\frac{1}{2}(n^2+2n+1)+\frac{1}{6}(n+1) =$$

$$= \frac{1}{3}n^3+n^2+n+\frac{1}{3}+\frac{1}{2}n^2+n+\frac{1}{2}+\frac{1}{6}n+\frac{1}{6} =$$

$$= \underbrace{\frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n}_{1^2+2^2+\dots+n^2} + \underbrace{n^2+2n+\frac{1}{3}+\frac{1}{2}+\frac{1}{6}}_{n^2+2n+1=(n+1)^2} \quad (=1) =$$

$$= 1^2+2^2+\dots+n^2+(n+1)^2 = L$$

□

Př. Dokažte, že pro libovolné přirozené číslo n je číslo n^3+2n dělitelné třemi.

1.) Ověříme platnost tvrzení pro $n = 1$:

$1^3 + 2 \cdot 1 = 1+2 = 3$, což je dělitelné číslem 3

2.) Provedeme indukční krok. Předpokládejme, že pro nějaké $n \in \mathbb{N}$ platí $n^3 + 2n = 3 \cdot k$, kde $k \in \mathbb{Z}$. Chceme dokázat, že potom také $(n+1)^3 + 2(n+1)$ je dělitelné třemi.

$$(n+1)^3 + 2(n+1) = n^3 + 3n^2 + 3n + 1 + 2n + 1 = \underbrace{n^3 + 2n}_{3 \cdot k} + 3n^2 + 3n + 3 =$$

$$= 3 \cdot (\underbrace{k + n^2 + n + 1}_{= K \in \mathbb{Z}})$$

Př. Matematickou indukcí dokažte, že $\forall n \in \mathbb{N}: \frac{2}{n} + \frac{4}{n} + \frac{6}{n} + \cdots + \frac{2n}{n} = n+1$

Důkaz: 1) Nejprve ověříme platnost tvrzení pro $n=1$

$$\frac{2}{n} = \frac{2}{1} = 2 = n+1 \quad V \qquad (2 = 2\cdot n)$$

Všimněme si, že rovnost platí i pro $n=2$, resp. $n=3$:

$$\frac{2}{2} + \frac{4}{2} = \frac{6}{2} = 3 = 2+1 \qquad (6 = 2\cdot 3)$$

resp. $\frac{2}{3} + \frac{4}{3} + \frac{6}{3} = \frac{12}{3} = 4 = 3+1$

2.) Provedeme indukční krok. Předpokládejme, že pro nějaké $n \in \mathbb{N}$ platí: $\frac{2}{n} + \frac{4}{n} + \frac{6}{n} + \cdots + \frac{2n}{n} = n+1$

chceme dokázat: $\underbrace{\frac{2}{n+1} + \frac{4}{n+1} + \frac{6}{n+1} + \cdots + \frac{2(n+1)}{n+1}}_{L} = \underbrace{(n+1)+1}_{P}$

$$L = \frac{1}{n+1} \cdot n \cdot \Big(\underbrace{\frac{2}{n} + \frac{4}{n} + \frac{6}{n} + \cdots + \frac{2n}{n}}_{= n+1 \text{ podle předpokladu}} + \frac{2(n+1)}{n} \Big) =$$

$$= \frac{1}{n+1} \cdot n \cdot \Big((n+1) + \frac{2(n+1)}{n} \Big) =$$

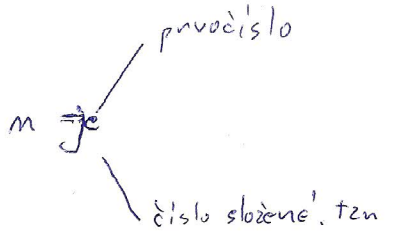
$$= n + 2 = (n+1) + 1 = P$$

Důkaz silnou matematickou indukcí: Dokazujeme výrok typu $\forall m \in \mathbb{N} : V(m)$

Postup:
1. Dokážeme: $V(1)$ platí
2. Dokážeme: $V(a)$ platí $\forall k \in \{1, 2, \dots, m-1\} \Rightarrow V(m)$ platí

Příklad: Věta: Každé přirozené číslo $m > 1$ je buď prvočíslo, nebo součin prvočísel.

Důkaz:
1. Dokážeme: $V(2)$ ← nejmenší přirozené číslo pro které má věta platit
   $V(2)$: $m = 2$ je prvočíslo, nebo součin prvočísel ✓
2. Předpokládejme, že každé číslo $k \in \{2, \dots, m-1\}$ je buď prvočíslo, nebo součin prvočísel. Snažíme se dokázat, že potom m je také buď prvočíslo, nebo součin prvočísel:



$m = a \cdot b$, kde ~~$a > 1$, $b > 1$~~

$1 < a < m$, $1 < b < m$

⇓

a i b jsou buď prvočísla, nebo jde o součin prvočísel

⇓

i m je součin prvočísel

$\Rightarrow$ m je buď prvočíslo, nebo součin prvočísel □