



**Katedra matematiky
PF UJEP**



Aritmetika s didaktikou I.

KM1 / 0001

Přednáška 08

Důkazy vět v teorii přirozených čísel

O čem budeme hovořit:

- Naučíme se provádět důkazy vět v teorii přirozených čísel pomocí axiomu indukce

Připomeňme si axiom indukce

$$(A7) \quad [F(0) \wedge (\forall x) (F(x) \Rightarrow F(x'))] \Rightarrow (\forall x) F(x)$$

Axiom se používá v důkazech obecných vět o přirozených číslech, které mají tvar $(\forall x) F(x)$.

Důkaz věty $(\forall x) F(x)$ bude mít vždy dva kroky:

1) ??? $F(0)$

2) ??? **jestliže platí $F(x)$, pak platí i $F(x')$**

(pro libovolné x)

Důkazy vět

Nejprve dokážeme tyto jednodušší věty o sčítání a násobení přirozených čísel

$$(V1) \quad (\forall x) \quad 0 + x = x$$

$$(V2) \quad (\forall x) \quad x + 1 = x'$$

$$(V3) \quad (\forall x) \quad 1 + x = x'$$

$$(V4) \quad (\forall x)(\forall y)(\forall z) \quad (x + y) + z = x + (y + z)$$

$$(V5) \quad (\forall x)(\forall y) \quad x + y = y + x$$

$$(V6) \quad (\forall x) \quad 0 \cdot x = 0$$

$$(V7) \quad (\forall x) \quad x \cdot 1 = x$$

$$(V8) \quad (\forall x)(\forall y)(\forall z) \quad x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(V1) \quad (\forall x) \quad 0 + x = x$$

Důkaz:

Formule $F(x)$ je $0 + x = x$.

1) ?? $F(0)$, tedy $0 + 0 = 0$. To plyne z (A3).

2) ?? $F(x) \Rightarrow F(x')$ pro libovolné x ,
tedy **jestliže** $0 + x = x$, **pak** $0 + x' = x'$.

Předpokladu $F(x)$, tj. $0 + x = x$ říkáme indukční předpoklad a budeme ho značit **IP**.

Dokazujeme tedy, že $0 + x' = x'$.

$$0 + x' = (0 + x)' = x' \\ (A4) \qquad (IP \text{ a } AI')$$



Číslo 0 je tedy neutrálním prvkem při sčítání.

$$(V2) \quad (\forall x) \quad x + 1 = x'$$

Důkaz:

Formule $F(x)$ je $x + 1 = x'$.

1) ?? $F(0)$, tedy $0 + 1 = 0'$.

Platí, že $0 + 1 = 1 = 0'$
(V1) (Def)

2) ?? $F(x) \Rightarrow F(x')$ pro libovolné x ,
tedy **jestliže** $x + 1 = x'$, **pak** $x' + 1 = (x')'$.

Dokazujme tedy, že $x' + 1 = (x')'$.

$$x' + 1 = x' + 0' = (x' + 0)' = (x')'$$

(Def)

(A4)

(A3 a AI')



$$(V3) \quad (\forall x) \quad 1 + x = x'$$

Důkaz:

Formule $F(x)$ je $1 + x = x'$.

1) ?? $F(0)$, tedy $1 + 0 = 0'$.

Platí, že $1 + 0 = 1 = 0'$
(A3) (Def)

2) ?? $F(x) \Rightarrow F(x')$ pro libovolné x ,
tedy **jestliže** $1 + x = x'$, **pak** $1 + x' = (x')'$.

Dokazujme tedy, že $1 + x' = (x')'$.

$$1 + x' = (1 + x)' = (x')'$$

(A4) (IP a AI')



$$(V4) \quad (\forall x)(\forall y)(\forall z) (x + y) + z = x + (y + z)$$

$$(\forall z)(\forall x)(\forall y) (x + y) + z = x + (y + z)$$

Důkaz:

Formule $F(z)$ je $(\forall x)(\forall y) (x + y) + z = x + (y + z)$

1) ?? $F(0)$, tedy $(\forall x)(\forall y) (x + y) + 0 = x + (y + 0)$.
 pro lib. x, y : $(x + y) + 0 = x + y = x + (y + 0)$.
 (A3) (A3 a AI+)

2) ?? $F(z) \Rightarrow F(z')$ pro libovolné z , tedy
 jestliže $(\forall x)(\forall y) (x + y) + z = x + (y + z)$,
 pak $(\forall x)(\forall y) (x + y) + z' = x + (y + z')$,
 pro libovolné x, y platí (proč?):
 $(x + y) + z' = [(x + y) + z]' = [x + (y + z)]' =$
 $= x + (y + z)' = x + (y + z')$. ■

$$(V5) \quad (\forall x)(\forall y) \quad x + y = y + x$$

$$(\forall y)(\forall x) \quad x + y = y + x$$

Důkaz:

Formule $F(y)$ je $(\forall x) \quad x + y = y + x$

1) ?? $F(0)$, tedy $(\forall x) \quad x + 0 = 0 + x$.

pro lib. x platí: $x + 0 = x = 0 + x$.

(A3) (V2)

2) ?? $F(y) \Rightarrow F(y')$ pro libovolné y , tedy

jestliže $(\forall x) \quad x + y = y + x$,

pak $(\forall x) \quad x + y' = y' + x$.

pro libovolné y platí (proč?):

$$x + y' = (x + y)' = 1 + (x + y) = 1 + (y + x) =$$

$$= (1 + y) + x = y' + x . \quad \blacksquare$$

$$(V6) \quad (\forall x) \quad 0 \cdot x = 0$$

Důkaz:

Formule $F(x)$ je $0 \cdot x = 0$.

1) ?? $F(0)$, tedy $0 \cdot 0 = 0$. To plyne z (A5).

2) ?? $F(x) \Rightarrow F(x')$ pro libovolné x ,
tedy **jestliže $0 \cdot x = 0$, pak $0 \cdot x' = 0$** .

Dokazujme tedy, že $0 \cdot x' = 0$.

$$0 \cdot x' = 0 \cdot x + 0 = 0 + 0 = 0$$

(A6)

(IP a AI+)

(A3)



Číslo 0 je tedy agresivním prvkem při násobení.

$$(V7) \quad (\forall x) \quad x \cdot 1 = x$$

Důkaz:

Formule $F(x)$ je $x \cdot 1 = x$.

1) ?? $F(0)$, tedy $0 \cdot 1 = 0$. To plyne z (V6).

2) ?? $F(x) \Rightarrow F(x')$ pro libovolné x ,
tedy **jestliže $x \cdot 1 = x$, pak $x' \cdot 1 = x'$** .

Dokazujeme tedy, že $x' \cdot 1 = x'$.

$$\begin{array}{ccccccc} x' \cdot 1 = & x' \cdot 0' = & x' \cdot 0 + x' = & 0 + x' = & x' \\ \text{(Def a AI.)} & \text{(A6)} & \text{(A5 a AI+)} & \text{(V1)} & \blacksquare \end{array}$$

Výsledek je jedním z tvrzení o tom, že číslo 1 je neutrálním prvkem při násobení.

$$(V8) \quad (\forall x)(\forall y)(\forall z) \ x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(\forall z)(\forall x)(\forall y) \ x \cdot (y + z) = x \cdot y + x \cdot z$$

Důkaz:

Formule $F(z)$ je $(\forall x)(\forall y) \ x \cdot (y + z) = x \cdot y + x \cdot z$

1) ?? $F(0)$, tedy $(\forall x)(\forall y) \ x \cdot (y + 0) = x \cdot y + x \cdot 0$.
pro libovolné x, y platí (proč?) :

$$x \cdot (y + 0) = x \cdot y = x \cdot y + 0 = x \cdot y + x \cdot 0$$

2) ?? $F(z) \Rightarrow F(z')$ pro libovolné z , tedy
jestliže $(\forall x)(\forall y) \ x \cdot (y + z) = x \cdot y + x \cdot z$
pak $(\forall x)(\forall y) \ x \cdot (y + z') = x \cdot y + x \cdot z'$.
pro libovolné x, y platí (proč?):

$$\begin{aligned} x \cdot (y + z') &= x \cdot (y + z)' = x \cdot (y + z) + x = \\ &= (x \cdot y + x \cdot z) + x = x \cdot y + (x \cdot z + x) = x \cdot y + x \cdot z' \quad \blacksquare \end{aligned}$$

Další možnosti

**Lze dokázat mnoho dalších vět o
přirozených číslech, například:**

$$(V9) \quad (\forall x)(\forall y)(\forall z) \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$(V10) \quad (\forall x)(\forall y) \ x' \cdot y = x \cdot y + y$$

$$(V11) \quad (\forall x)(\forall y) \ x \cdot y = y \cdot x$$

$$(V12) \quad (\forall x)(\forall y)(\forall z) \ x + z = y + z \Rightarrow x = y$$

$$(V13) \quad (\forall x)(\forall y) \ x + y = 0 \Rightarrow x = 0 \wedge y = 0$$

$$(V14) \quad (\forall x)(\forall y)(\forall z) \ x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$$

$$(V15) \quad (\forall x)(\forall y) \ x \cdot z = y \cdot z \wedge z \neq 0 \Rightarrow x = y$$

Definice relací $\leq$ a $<$.

Definice:

$$x \leq y \Leftrightarrow_D (\exists z) x + z = y$$

Relaci $x \leq y$ čteme „ x je menší nebo rovno y “.

Definice:

$$x < y \Leftrightarrow_D (\exists z) x + z = y \wedge z \neq 0$$

Relaci $x < y$ čteme „ x je menší než y “.

Lze dokázat další fakta o právě definovaných relacích, například:

$\text{Relace} \leq$ je neostré lineární uspořádání.

$\text{Relace} <$ je ostré lineární uspořádání.

$\text{Relace} \leq$ je invariantní vzhledem k operaci sčítání.

$\text{Relace} \leq$ je invariantní vzhledem k operaci násobení.

$\text{Relace} <$ je invariantní vzhledem k operaci sčítání.

$\text{Relace} <$ není invariantní vzhledem k operaci násobení.

atd.

Děkuji za pozornost

