Matematická indukce II – Recept na přirozená čísla

Milý příteli,

vítáme Tě u druhého dílu seriálu o matematické indukci! Možná sis všiml(a), že většina cvičení z minulého dílu počítá s přirozenými čísly. Často jsme chtěli dokázat, že nějaké tvrzení platí pro všechna přirozená čísla. Už samotný princip indukce je definovaný na přirozených číslech. Proto si v tomto díle položíme otázku, co jsou to vlastně ta přirozená čísla, a podíváme se na ně úplně od základů! Začneme axiomy, které definují přirozená čísla, a pouze na jejich základě odvodíme operace na přirozených číslech, jako je sčítání či násobení.

Tento díl se od prvního dílu liší tím, že při čtení je třeba mnohem víc abstraktního myšlení a pochopení některých zcela nových konceptů. V textu najdeš jednu velmi důležitou větu, nazvanou věta o rekurzi, kterou posléze využijeme k definování operací na přirozených číslech. Její důkaz je poměrně technický a nevadí, pokud se budeš místy ztrácet, pro pochopení dalšího textu nutný není.

Podnětné čtení Ti přejí

Káťa a Ittihad

Úvod

Bůh stvořil přirozená čísla, všechno ostatní je lidské dílo.
– Leopold Kronecker (1823–1891)

Odbočme nyní zdánlivě od tématu indukce a položme si otázku: Co jsou to přirozená čísla?

Můžeme je vyjmenovat: 1, 2, 3 a tak dále, každé další číslo je o 1 větší než to předchozí. Jenže tento seznam nám nic neřekne o jejich vlastnostech – jak funguje sčítání či násobení přirozených čísel? Máme-li dvě přirozená čísla, umíme je porovnat? Co víc, nelze vypsat všechna přirozená čísla – víme tedy, jak vypadají a jak se chovají velmi vysoká čísla? Je tento seznam opravdu nekonečný?

K samotnému vyjmenování přirozených čísel jsme potřebovali frázi „a tak dále“. V minulém díle jsme zjistili, že na argumentu „a tak dále“ vlastně stojí celý důkaz matematickou indukcí. Celou dobu jsme ovšem mlčky předpokládali, že všechna přirozená čísla lze takto induktivně pokrýt, žádnou záruku, že to jde, jsme však nedostali!

Aby naše důkazy nestály na zavádějícím a nejasném „a tak dále“, zahrneme matematickou indukci *přímo do definice* přirozených čísel.

Nejprve však zavedeme několik užitečných pojmů.

Funkce

If you are wandering down in Cornmarket and you bump into a second-hand function dealer and they try to sell you a function with only the rule part and not the domain or the codomain, please walk away! They're a dodgy, unscrupulous function dealer and you should not trade with them.
– Vicky Neale (University of Oxford)

Definice. *Zobrazení* f množiny A do množiny B je cokoli, co každému prvku a množiny A přiřadí právě jeden prvek množiny B. Ten pak značíme $f(a)$.

Zobrazení může být zadáno nějakým pravidlem, například zobrazení, které každému reálnému číslu x přiřadí jeho obraz x^2. Můžeme ale narazit i na zobrazení z množiny $\{1, 3, 7\}$ do množiny $\{2, 3, 4, 10\}$, které jedničce přiřadí 10, trojce přiřadí 4 a sedmičce přiřadí 10. Navíc množiny A a B ani nemusí být množiny čísel, ale např. množiny trojúhelníků v rovině, zvířat v zoo, žáků 3.B atd.

Termín *cokoli* v předchozí definici se může zdát poněkud vágní. Zobrazení neboli funkci můžeme přesněji definovat pomocí množin – představme si, že naše funkce páruje prvky množiny A s prvky z B. Výčtem uspořádaných dvojic $(a, f(a))$ pak funkci f jasně popíšeme. Množinu všech uspořádaných dvojic (a, b), kde $a \in A$ a $b \in B$ nazýváme kartézským součinem a značíme ji $A \times B$. To inspiruje následující definici:

Definice. Nechť jsou A a B množiny. *Funkce* $f\colon A \to B$ je taková *podmnožina* f množiny $A \times B$, pro kterou platí

(i) pro všechna $a \in A$ existuje $b \in B$ takové, že $(a, b) \in f$,
(ii) tento prvek b je právě jeden, tedy pokud $(a, b) \in f$ a současně $(a, c) \in f$, potom $b = c$.

Poznámka. Důležité je, že funkce f vždy „chodí společně“ s množinami A a B! Je důležité uvést, odkud a kam funkce posílá prvky.[1]

Ukážeme si to na příkladu funkce $f\colon \mathbb{R} \to \mathbb{R}$ dané předpisem $f(x) = x^2$. Zde bychom funkci popsali pomocí uspořádaných dvojic (x, x^2) pro každé $x \in \mathbb{R}$. Tyto dvojice můžeme znázornit grafem funkce, který znáte ze školy – každý bod paraboly odpovídá jedné z dvojic. Mezi dvojicemi, které popisují naši funkci, by byly například $(0, 0)$, $(1, 1)$, $(2, 4)$, ale i $(-1, 1)$ nebo $(-5, 25)$.

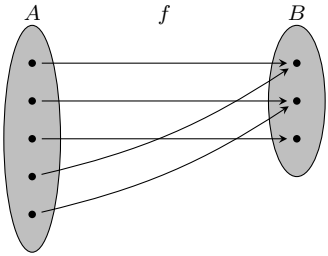
Cvičení 1. Kolik existuje funkcí z množiny $A = \{1, 2, 3\}$ do množiny $B = \{0, 1\}$?

Podotkněme, že není nutné, aby všechny prvky množiny B byly použity. Stejně tak není nutné, aby byly prvkům množiny A přiřazeny různé prvky množiny B. To vede k následujícím definicím:

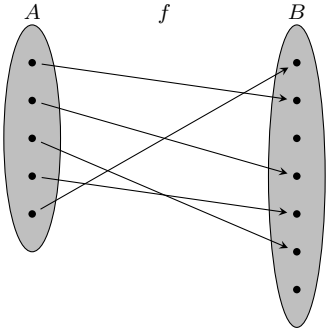
[1] Viz citát výše.

Definice. Nechť $f\colon A \to B$ je funkce. Potom:

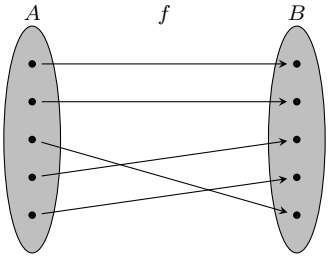
(i) f je *na*, pokud pro každé $b \in B$ existuje $a \in A$ takové, že $f(a) = b$.



(ii) f je *prostá*, jestliže pro všechna $x, y \in A$ platí, že pokud $f(x) = f(y)$, tak nutně $x = y$.



(iii) f je *bijekce*, pokud je zároveň prostá a na.



Peanovy axiomy

Mathematical induction is a definition, not a principle.
– Bertrand Russell (1872–1970)

Naším cílem v této kapitole bude definovat přirozená čísla. Velmi zajímavé a možná na první pohled zarážející je to, že přirozená čísla definuje právě možnost dělat na nich indukci. Všechny další

vlastnosti, jako je způsob počítání s přirozenými čísly nebo jejich pořadí, potom z této vlastnosti vyplývají.

Bude se nám hodit pracovat i s nulou jako přirozeným číslem, proto rozšiřme množinu $\mathbb{N}$ na množinu přirozených čísel s nulou, kterou označíme $\mathbb{N}_0$. Ve zbytku textu budeme nulu považovat za přirozené číslo.

Přirozená čísla po sobě následují. Začneme nulou, pokaždé přičteme 1 a opakujeme. Tuto vlastnost chceme zahrnout do definice.

Zavedeme proto funkci $s\colon \mathbb{N}_0 \to \mathbb{N}_0$, kterou nazveme *následník*[2], jež bude vystihovat to, že jedno číslo následuje po jiném, tedy $s(1) = 2$, $s(2) = 3$ a podobně.

Zamysleme se nad tím, co bychom od této funkce chtěli, aby nám definovala přirozená čísla. Zaprvé, číslo 0 není následníkem žádného čísla. Zadruhé, známe-li následníka nějakého čísla, je toto číslo už jednoznačně určeno (neboli dvě různá čísla nemohou mít stejného následníka). Zatřetí, tato funkce musí mít určitou vlastnost, kterou využijeme při indukci. Při důkazu matematickou indukcí jsme nejprve ukázali, že tvrzení platí pro 0 a poté jsme dokázali, že platí-li pro n, tak platí i pro $n+1$. Tím byl důkaz završen – tvrzení platí pro všechna přirozená čísla. Něco podobného vyslovme v jazyce množin, vždyť přirozená čísla jsou také množina:

„Předpokládejme, že S je podmnožina $\mathbb{N}_0$, která obsahuje nulu a pro kterou platí, že pokud $n \in S$, tak i $s(n) \in S$. Potom $S = \mathbb{N}_0$."

Ukáže se, že pouhé tyto tři vlastnosti naprosto stačí k jednoznačné definici přirozených čísel!

Představíme *Peanovy axiomy*, které pro definování množiny přirozených čísel zavedl italský matematik konce 19. století Giuseppe Peano.

Peanovy axiomy. *Předpokládejme, že existuje množina $\mathbb{N}_0$ a funkce $s\colon \mathbb{N}_0 \to \mathbb{N}_0$ taková, že:*

(1) *Funkce s není na: existuje prvek $0 \in \mathbb{N}_0$ takový, že pro žádné $n \in \mathbb{N}_0$ neplatí $s(n) = 0$.*
(2) *Funkce s je prostá: je-li $s(m) = s(n)$, potom $m = n$.*
(3) *Je-li S podmnožina $\mathbb{N}_0$ taková, že $0 \in S$ a pro všechna $n \in \mathbb{N}_0$ platí $n \in S \implies s(n) \in S$, potom $S = \mathbb{N}_0$.*

Poznámka. Všimněme si, že $s\colon \mathbb{N}_0 \to \mathbb{N}_0$ znamená, že pro přirozené číslo n platí, že jeho následník $s(n)$ je také přirozené číslo, tedy množina $\mathbb{N}_0$ je *uzavřená na operaci s*.

Nic nám nezaručuje, že daná množina skutečně existuje, proto vezmeme její existenci jako axiom neboli tvrzení, které považujeme za pravdivé a nedokazujeme jej. Je to jako můstek, od kterého se musíme odrazit, chceme-li vůbec nějak dál v matematice pracovat.

Axiom. (existence přirozených čísel) *Existuje množina $\mathbb{N}_0$ a funkce $s\colon \mathbb{N}_0 \to \mathbb{N}_0$, které splňují Peanovy axiomy výše.*

Z 2. axiomu plyne, že různá čísla mají různé následníky. Proto pokud číslo má předchůdce, pak je jen jeden. Která čísla ovšem mají předchůdce mají?

Tvrzení. *Pro každé $n \in \mathbb{N}_0$ různé od 0 existuje právě jedno $m \in \mathbb{N}_0$ takové, že $n = s(m)$.*

Důkaz. Chceme ukázat, že pro libovolné $n \in \mathbb{N}_0$ je buď $n = 0$, nebo $n = s(m)$ pro nějaké $m \in \mathbb{N}_0$. Využijeme k tomu třetí Peanův axiom a indukci, a to tak, že sestrojíme množinu S obsahující ta čísla n, pro která to platí, a pak ukážeme, že $S = \mathbb{N}_0$.

Nechť $S = \{n \in \mathbb{N}_0;\ n = 0 \text{ nebo } n = s(m) \text{ pro nějaké } m \in \mathbb{N}_0\}$. Jistě platí, že $0 \in S$. Nyní předpokládejme, že číslo n je v S, a pokusme se ukázat, že potom je i $s(n)$ v S. Co lze říct o číslu $s(n)$? Jistě $s(n) = s(m)$ pro nějaké $m \in \mathbb{N}_0$, konkrétně pro $m = n$. Tedy $s(n) \in S$. Podle třetího Peanova axiomu pak platí, že $S = \mathbb{N}_0$, což jsme chtěli ukázat. □

[2] Anglicky je to *successor*, a proto ji značíme s.

Aritmetika

Označení *přirozená čísla* zřejmě pochází z lidské zkušenosti – již starověké civilizace používaly právě čísla 1, 2, ... k počítání každodenních věcí, měření délek a porovnávání množství. Tato čísla se prostě používala k zacházení s přirozeně se vyskytujícími jevy. Např. záporná čísla do tohoto konceptu nepatřila, neboť nelze mít méně než nic (záporné množství lidé ještě neuvažovali), o racionálních, iracionálních či komplexních číslech ani nemluvě.

Přirozená čísla se tedy vyvinula jako čísla používaná k počítání. K tomu budeme potřebovat dvě základní operace, sčítání a násobení.

Uvažme nejprve sčítání. Mějme dva košíky jablek, v jednom 10 a ve druhém 7 kusů ovoce. Představme si, že zatím neumíme sčítat z paměti. Jak zjistíme, kolik jablek máme dohromady? Nejprve spočítáme jablka v prvním košíku, 1, 2, ..., 10, poté bereme do ruky jedno jablku z druhého košíku po druhém a pokračujeme přitom s vyjmenováváním čísel 11, 12, ..., 17. Navíc víme-li, jak přičíst číslo 7, potom umíme přičíst i číslo 8 – prostě přidáme jedno jablko. Na základě této zkušenosti bychom rádi definovali sčítání takto:

$$m + (n + 1) = (m + n) + 1.$$

Jedná se o rekurzivní definici – víme-li, jak přičíst n, tak víme i to, jak přičíst $n + 1$.

Potřebujeme ovšem ještě nějaký základní kámen, od kterého se odrazíme. Tím pro nás bude přičítání nuly, tedy vlastnost, že nepřidáme-li žádné jablko, počet jablek se nezmění.

$$m + 0 = m.$$

Je tu ovšem jistý zádrhel: Zaprvé, abychom k číslu m přičetli $n+1$, potřebujeme již znát hodnotu $m + n$. Tu můžeme získat postupným přičítáním jednotek k číslu m, dokud se nedostaneme na hodnotu n. To je intuitivní přístup, v naší definici podle Peanových axiomů ovšem není řečeno, zda se takto vůbec někdy dobereme čísla n.

Abychom dali rekurzivní definici pevný rámec a zároveň se vyhnuli slovnímu spojení „a tak dále, dokud nenarazíme na n“, dokážeme si následující větu pro obecný případ, kterou poté aplikujeme ve vhodných podmínkách.

Věta. (o rekurzi) *Mějme množinu X a funkci $f\colon X \to X$. Nechť $c \in X$. Potom existuje právě jedna funkce $\varphi\colon \mathbb{N}_0 \to X$ taková, že*

(1) $\varphi(0) = c$,
(2) $\varphi(s(n)) = f(\varphi(n))$ *pro každé* $n \in \mathbb{N}_0$.

Poznámka. Funkce φ nám tedy říká, kolikrát jsme aplikovali funkci f na prvek c, jedná se o opakovanou kompozici funkce f. Máme

$$\varphi(n) = f^n(c) = \underbrace{f(f(\cdots f(}_{n\text{-krát}} c)\cdots)).$$

Chceme ukázat to, že taková funkce existuje a že je jen jedna (pro dané f a c). Když později nahradíme f funkcí s, potvrdíme tak, že rekurzivní definice sčítání dává smysl neboli že je *dobře definovaná*.

Důkaz. Nejprve se ohlédněme a vzpomeňme si, co je to funkce. Funkci jsme si zadefinovali jako množinu uspořádaných dvojic, která splňuje dva požadavky: každý prvek vstupní množiny je v nějaké dvojici a tato dvojice je jedinečná.

My navíc potřebujeme, aby funkce φ splňovala body (1) a (2), tedy aby byla takovou podmnožinou $\mathbb{N}_0 \times X$, že

(1) $(0, c) \in \varphi$,
(2) pokud $(n, x) \in \varphi$, tak také $(s(n), f(x)) \in \varphi$.

Podmnožin splňujících body (1) a (2) (které však nemusí být funkce) je mnoho, např. i celá množina $\mathbb{N}_0 \times X$. My ukážeme, že ta, kterou hledáme (tj. která bude zároveň funkcí), je průnikem všech podmnožin splňujících body (1) a (2). Jinými slovy to znamená, že naše hledaná podmnožina je nejmenší možná.

Nechť φ je průnikem všech podmnožin $U \subset \mathbb{N}_0 \times X$, pro které platí

(1) $(0, c) \in U$
(2) pokud $(n, x) \in U$, tak také $(s(n), f(x)) \in U$.

Nejprve ukážeme, že se jedná o funkci. To znamená ukázat, že pro každé $n \in \mathbb{N}_0$ existuje právě jedno $x \in X$ takové, že $(n, x) \in \varphi$. Ukážeme to pomocí indukce, tedy s využitím třetího Peanova axiomu.

Nechť $S = \{n \in \mathbb{N}_0;\ (n, x) \in \varphi$ pro nějaké $x \in X\}$ je množina všech přirozených čísel, pro která existuje nějaká funkční hodnota x. Podle první podmínky je $0 \in S$. Nyní pokud $n \in S$, tak existuje $x \in X$, pro které $(n, x) \in \varphi$, a proto podle druhé podmínky také $(s(n), f(x)) \in \varphi$. Jelikož $f(x) \in X$, získáváme $s(n) \in S$ a induktivně podle třetího axiomu pak $S = \mathbb{N}_0$.

Tedy pro každé $n \in \mathbb{N}_0$ existuje alespoň jedna dvojice (n, x). Chceme ukázat, že tato dvojice je jen jedna, což bude znamenat, že φ definuje funkci. K tomu využijeme podmínku, že φ je průnikem všech podmnožin $\mathbb{N}_0 \times X$, které splňují (1) a (2).

Nechť $T = \{n \in \mathbb{N}_0;\ (n, x) \in \varphi$ pro právě jedno $x \in X\}$ je množina všech přirozených čísel, pro něž existuje jedinečná funkční hodnota x. Ověříme, že $T = \mathbb{N}_0$.

Nejprve ukážeme, že $0 \in T$. Pro spor předpokládejme, že existuje $d \neq c$, pro které $(0, d) \in \varphi$. Uvažme množinu $\varphi^* = \varphi \setminus \{(0, d)\}$. Potom $(0, c) \in \varphi^*$, a pokud $(n, x) \in \varphi^*$, tak $(s(n), f(x)) \in \varphi^*$. To platí, protože $(s(n), f(x))$ rozhodně není odebranou dvojicí $(0, d)$, jelikož $0 \neq s(n)$ pro žádné $n \in \mathbb{N}_0$. Jenže $\varphi^* \subset \varphi$ splňuje podmínky (1) a (2), což je ve sporu s předpokladem, že φ je průnikem všech takových podmnožin. Tedy $0 \in T$.

Obdobně ukážeme, že pokud $n \in T$, tak také $s(n) \in T$. Předpokládejme tedy, že $(n, x) \in \varphi$ pro jedno jediné $x \in X$. Potom podle (2) platí $(s(n), f(x)) \in \varphi$. Pro spor nechť existuje $y \neq f(x)$ takové, že $(s(n), y) \in \varphi$. Sestrojme tentokrát $\varphi^* = \varphi \setminus \{(s(n), y)\}$. Potom $(0, c) \in \varphi^*$. Mějme $(m, z) \in \varphi^*$. Chceme ukázat, že potom $(s(m), f(z)) \in \varphi^*$. Buď $m = n$, potom $z = x$ a víme, že $(s(m), f(z))$ ve φ^* leží. Nebo platí $m \neq n$. V tom případě $(s(m), f(z)) \in \varphi^*$, protože $(s(m), f(z)) \in \varphi$ podle (2) a zároveň $s(m) \neq s(n)$ podle 2. axiomu, takže jsme tuto dvojici nemohli vyhodit jako $(s(n), y)$. V každém případě pro φ^* platí (2), což je spor s tím, že φ je nejmenší podmnožinou splňující body (1) a (2).

Z toho plyne, že pokud $n \in T$, tak také $s(n) \in T$. Potom podle třetího axiomu $T = \mathbb{N}_0$.

Dokázali jsme, že takto sestrojené φ je funkce, která splňuje podmínky věty o rekurzi. Navíc tato funkce je jen jedna. Předpokládejme totiž, že máme jinou funkci ψ, která také řeší naše zadání. Potom je z definice naše sestrojená funkce φ podmnožinou ψ. Ale z funkce nelze už nic škrtnout, jinak by nebyla definovaná na celém oboru, a proto $\varphi = \psi$. Tím jsme hotovi. □

K čemu nám věta o rekurzi bude? Už dříve jsme naťukli, že součet dvou čísel můžeme definovat pomocí opakovaného přičítání čísla 1. Dosaďme za f funkci následník s a za c nějaké počáteční číslo. Potom funkci φ můžeme chápat jako operaci „přičti to k danému číslu c“. Druhá část věty o rekurzi se pak přemění na tvrzení „nejprve vzít následníka čísla n a poté ho přičíst je stejné, jako nejprve přičíst číslo n a poté vzít následníka součtu“. Pokud tedy za f vezmeme funkci následník s, pak nám věta o rekurzi říká, že součet, kterého se takto dobereme, je právě jeden. To je důležité, protože když definujeme operaci, musíme se ujistit, že nám ta operace vyhodí právě jeden výsledek.

Poznámka. Pro lepší pochopení toho, co se myslí pojmem „dobře definovaná operace“, zabrousíme do počítání modulo 3. Nejde o nic jiného, než že číslo n nahradíme jeho zbytkem po dělení 3.

Toto číslo pak značíme n_3.[3] Např. $32_3 = 2_3$ a $4_3 = 1_3$. Představme si, že bychom rádi definovali mocnění modulo 3. Intuitivně zkusíme definovat

$$(m_3)^{n_3} = (m^n)_3,$$

tedy že vezmeme-li dvě čísla m a n, pak dostaneme stejný výsledek, když nejprve vezmeme zbytky těch čísel a umocníme, jako když nejprve umocníme a potom vezmeme zbytek. Ovšem potom

$$1_3 = 4_3 = (2^2)_3 = (2_3)^{2_3} = (2_3)^{5_3} = (2^5)_3 = 32_3 = 2_3,$$

což je zjevný nesmysl – umocněním čísla 2_3 postupně na čísla 2_3 a 5_3 jsme dostali různé výsledky, přitom však $2_3 = 5_3$, a tedy bychom měli získat stejný výsledek. Toto se stalo právě proto, že naše operace nebyla dobře definovaná.

Nyní můžeme definovat mnohé rekurzivní operace na přirozených číslech pro dané $m \in \mathbb{N}_0$.

(1) *Sčítání* $\alpha_m \colon \mathbb{N}_0 \to \mathbb{N}_0$.
Operace sčítání je definována rekurzivně takto:

$$\begin{aligned} \alpha_m(0) &= m, \\ \alpha_m(s(n)) &= s(\alpha_m(n)). \end{aligned}$$

Budeme používat běžné značení $\alpha_m(n) = m+n$, a proto předchozí dvě rovnosti lze přeložit jako $m + 0 = m$ a $m + (n + 1) = (m + n) + 1$.

K tomu, aby bylo sčítání dobře definované, jsme využili větu o rekurzi s $c = m$ a $f = s$.

(2) *Násobení* $\mu_m \colon \mathbb{N}_0 \to \mathbb{N}_0$.
Násobení rekurzivně definujeme pomocí

$$\begin{aligned} \mu_m(0) &= 0, \\ \mu_m(s(n)) &= \mu_m(n) + m. \end{aligned}$$

Tentokrát jsme ve větě o rekurzi položili $c = 0$ a $f(x) = x + m$.

Násobení zapisujeme jako obvykle $\mu_m(n) = mn$. Použitím tohoto zápisu na předchozí dvě rovnice dostaneme $m \cdot 0 = 0$ a $m(n + 1) = mn + m$.

Všimněme si, že k samotné definici násobení jsme potřebovali mít už zadefinované sčítání.

(3) *Mocnění* $\pi_m \colon \mathbb{N}_0 \to \mathbb{N}_0$.
Mocniny definujeme rekurzivně pomocí

$$\begin{aligned} \pi_m(0) &= 1, \\ \pi_m(s(n)) &= m\pi_m(n). \end{aligned}$$

Zde jsme položili $c = 1$ a $f(r) = rm$.

Běžně zapisujeme $\pi_m(n) = m^n$, a mocnění je tedy definováno podle $m^0 = 1$ a $m^{(n+1)} = m \cdot m^n$.

Opět si uvědomme, že v definici předpokládáme, že násobení je už definováno.

[3] Toto značení není obecně moc rozšířené.

Máme definované základní operace na přirozených číslech a je čas dokázat některá základní „pravidla“ pro jejich používání. Tyto zásady běžně používáme. A nyní nás vlastně čeká ukázat, že tato pravidla nejsou ve své podstatě pravidla, nýbrž důsledky Peanových axiomů!

Nejprve nahradíme zápis pomocí funkce následník $s(n)$ běžnějším značením $n+1$. Dostaneme tak rekurzivní definice sčítání a násobení

$$\begin{aligned} &(\alpha 1) \quad m+0=m, && (\alpha 2) \quad m+(n+1)=(m+n)+1,\\ &(\mu 1) \quad m0=0, && (\mu 2) \quad m(n+1)=mn+m. \end{aligned}$$

Důkazy základních pravidel využívají indukci neboli třetí Peanův axiom. Ukážeme si to nejprve na příkladu.

Tvrzení. *Platí*

$$\begin{aligned} &(a) \quad 0+m=m,\\ &(b) \quad 1+m=m+1,\\ &(c) \quad 0m=0,\\ &(d) \quad 1m=m. \end{aligned}$$

Důkaz. (a) Použijeme indukci podle m. Nechť $S=\{m\in\mathbb{N}_0;\ 0+m=m\}$.

Potom $0\in S$, neboť $0+0=0$ podle $(\alpha 1)$. Dále pokud $m\in S$, tak

$$0+(m+1)=(0+m)+1=m+1$$

podle $(\alpha 2)$, tedy $m+1\in S$. Z 3. axiomu potom plyne $S=\mathbb{N}_0$, a tedy $0+m=m$ pro všechna $m\in\mathbb{N}_0$.

(b) Buď $S=\{m\in\mathbb{N}_0;\ 1+m=m+1\}$. Potom

$$\begin{aligned} 1+0&=1 && \text{podle } (\alpha 1)\\ &=0+1 && \text{podle } (a), \end{aligned}$$

takže $0\in S$.

Předpokládejme, že $m\in S$. Potom

$$\begin{aligned} 1+(m+1)&=(1+m)+1 && \text{podle } (\alpha 2)\\ &=(m+1)+1 && \text{podle indukčního předpokladu,} \end{aligned}$$

a tedy i $m+1\in S$. Podle třetího axiomu pak dostáváme $S=\mathbb{N}_0$, neboli $1+m=m+1$ pro všechna $m\in\mathbb{N}_0$.

Cvičení 2. Dokaž si sám (sama) body (c) a (d). □

Asociativita

Tvrzení. *Pro všechna* $m,n,p\in\mathbb{N}_0$ *platí*

$$(m+n)+p=m+(n+p).$$

Ukážeme, že operace $+$ je asociativní, což ve volném překladu znamená „zapomeňte na závorky“. Díky této vlastnosti později budeme moct psát prostě $m+n+p$ a budeme vědět, že nezáleží na tom, zda nejprve sečteme m a n a potom přičteme p, nebo zda k m přičteme součet $n+p$.

Důkaz. Důkaz provedeme indukcí podle p. Mějme libovolná, avšak pevně stanovená čísla m a n. Nechť

$$S=\{p\in\mathbb{N}_0;\ (m+n)+p=m+(n+p)\}.$$

Potom $0 \in S$, protože

$$\begin{aligned}(m+n)+0 &= m+n && \text{podle } (\alpha 1)\\ &= m+(n+0) && \text{podle } (\alpha 1).\end{aligned}$$

Nyní jestliže $p \in S$, potom

$$\begin{aligned}(m+n)+(p+1) &= ((m+n)+p)+1 && \text{podle } (\alpha 2)\\ &= (m+(n+p))+1 && \text{podle indukčního předpokladu}\\ &= m+((n+p)+1) && \text{podle } (\alpha 2)\\ &= m+(n+(p+1)) && \text{podle } (\alpha 2),\end{aligned}$$

takže $p+1 \in S$.

Potom třetí axiom říká, že $S = \mathbb{N}_0$, a tedy $(m+n)+p = m+(n+p)$ pro všechna $m, n, p \in \mathbb{N}_0$, jak jsme chtěli ukázat. □

Poznámka. Všimněte si, že pro první část důkazu jsme potřebovali pouze $(\alpha 1)$, kdežto pro indukční krok jsme již využili $(\alpha 2)$.

Komutativita

Tvrzení. *Pro všechna $m, n \in \mathbb{N}_0$ máme*

$$m+n = n+m.$$

To, že je operace $+$ komutativní, znamená, že můžeme prohodit pořadí sčítanců. Zdá se to jako jasná věc – jako výstraha, proč je potřeba to dokázat, nám poslouží příklad operace, která není komutativní, například odčítání nebo dělení, zde na pořadí záleží!

Důkaz. Použijeme indukci na n. Mějme $m \in \mathbb{N}_0$ a sestrojme množinu

$$S = \{n \in \mathbb{N}_0;\ m+n = n+m\}.$$

Nyní podle $(\alpha 1)$ a (a) víme, že $0 \in S$. Dále pokud platí $m+n = n+m$, tak

$$\begin{aligned}m+(n+1) &= (m+n)+1 && \text{podle } (\alpha 2)\\ &= (n+m)+1 && \text{podle indukčního předpokladu}\\ &= 1+(n+m) && \text{podle } (b)\\ &= (1+n)+m && \text{díky asociativitě sčítání}\\ &= (n+1)+m && \text{podle } (b),\end{aligned}$$

a proto $n+1 \in S$. Z třetího Peanova axiomu pak vyplývá, že $S = \mathbb{N}_0$, a tedy pro všechna $m, n \in \mathbb{N}_0$ platí $m+n = n+m$, čímž jsme hotovi. □

Poznámka. Znovu si všimněme, které předchozí vlastnosti jsme použili. Tentokrát jsme potřebovali také (a) a (b), na rozdíl od důkazu asociativity, a také byla zapotřebí asociativita samotná. Proto bývá výhodné najít vhodné pořadí pro dokazování tvrzení, na což ještě narazíme.

Distributivita

Tvrzení. *Pro všechna $m, n, p \in \mathbb{N}_0$ platí*

$$m(n+p) = mn+mp.$$

Distributivitě násobení přes sčítání často říkáme „roznásobení závorky“. I tato vlastnost je dokazatelná na základě tří Peanových axiomů.

Důkaz. Budeme postupovat indukcí podle p. Pro daná $m, n \in \mathbb{N}_0$ označme

$$S = \{p \in \mathbb{N}_0;\ m(n+p) = mn + mp\}.$$

Nejprve ukážeme, že $0 \in S$. Máme

$$\begin{aligned} m(n+0) &= mn && \text{podle } (\alpha 1)\\ &= mn + 0 && \text{podle } (\alpha 1)\\ &= mn + m0 && \text{podle } (\mu 1). \end{aligned}$$

Nyní předpokládejme, že $p \in S$. Potom

$$\begin{aligned} m(n+(p+1)) &= m((n+p)+1) && \text{podle } (\alpha 2)\\ &= m(n+p) + m && \text{podle } (\mu 2)\\ &= (mn + mp) + m && \text{podle indukčního předpokladu}\\ &= mn + (mp + m) && \text{díky asociativitě}\\ &= mn + m(p+1) && \text{podle } (\mu 2), \end{aligned}$$

a tedy $p + 1 \in S$. Podle třetího axiomu pak máme, že $S = \mathbb{N}_0$, a tedy pro všechna $m, n, p \in \mathbb{N}_0$ platí distributivní zákon. □

Poznámka. Poznamenejme, že k důkazu jsme kromě rekurzivních definic sčítání a násobení potřebovali také asociativitu, kterou již máme dokázanou.

Násobení

Zbývá nám ukázat asociativitu a komutativitu násobení.

Úloha 1. Ukaž, že pro všechna $m, n, p \in \mathbb{N}_0$ platí $m(np) = (mn)p$.

Důkaz následujícího tvrzení je o něco důvtipnější a zajímavější.

Tvrzení. *Pro všechna $m, n \in \mathbb{N}_0$ platí komutativní zákon $mn = nm$.*

Důkaz. Mějme pro dané $m \in \mathbb{N}_0$

$$S = \{n \in \mathbb{N}_0;\ mn = nm\}.$$

Podle (c) je 0 v S. Nyní jestliže $n \in S$, tak

$$\begin{aligned} m(n+1) &= mn + m && \text{podle } (\mu 2)\\ &= nm + m && \text{díky komutativitě.} \end{aligned}$$

Nyní přijde ta hustokrutopřísná část. Hodilo by se nám, kdybychom mohli vytknout m „dozadu“, to bohužel ještě nevíme. Ovšem vzhledem k tomu, že jsme už ukázali vytýkání „dopředu“ neboli distributivitu, můžeme se právem domnívat, že půjde něco obdobného i opačně. Klíčem k tomu je další indukce. Ať

$$T = \{m \in \mathbb{N}_0;\ nm + m = (n+1)m\}.$$

Zjevně $0 \in T$. Dále pokud $m \in T$, tak

$$\begin{aligned}
n(m+1)+(m+1) &= (nm+n)+(m+1) && \text{podle } (\mu 2)\\
&= nm+n+m+1 && \text{díky asociativitě můžeme rozpustit závorky}\\
&= nm+m+n+1 && \text{díky komutativitě sčítání lze přeuspořádat členy}\\
&= (nm+m)+(n+1) && \text{díky asociativitě můžeme závorkovat, jak chceme}\\
&= (n+1)m+(n+1) && \text{podle indukčního předpokladu}\\
&= (n+1)(m+1) && \text{podle } (\mu 2).
\end{aligned}$$

Tedy $m+1 \in T$ a podle třetího axiomu $T = \mathbb{N}_0$. Konečně tedy dostáváme, že $m(n+1) = (n+1)m$, a tedy $n+1 \in S$. Podle třetího Peanova axiomu potom $S = \mathbb{N}_0$ a $mn = nm$ pro všechna $m, n \in \mathbb{N}_0$, jak jsme chtěli ukázat. □

Porovnávání

Kromě sčítání a násobení můžeme přirozená čísla také porovnávat. Jak definujeme, že a je menší nebo rovno b? Můžeme se na to podívat tak, že seřadíme přirozená čísla do řady podle toho, jak po sobě *následují*, a řekneme, že a je menší nebo rovno b, pokud je a v řadě dříve (nebo nastejno) než b. Jenže pokud jsou čísla a nebo b velmi vysoká, tak bychom se k nim také nemuseli za lidský život dopracovat. Zkusme jiný pohled, řekněme, že $a \leq b$, pokud je rozdíl $b - a$ také přirozeným číslem. Avšak rozdíl jsme ještě nedefinovali, navíc se dostáváme k definici kruhem, kdy rozdíl $b - a$ dvou přirozených čísel můžeme vůbec definovat jen tehdy, když $a \leq b$, protože záporná čísla vlastně ještě neznáme. Tento zádrhel však můžeme snadno obejít tak, že definujeme $a \leq b$ právě tehdy, když existuje přirozené číslo r takové, že $b = a + r$. Číslo r je tu tím nezáporným rozdílem.

Definice. Definujme relaci $\leq$ na množině přirozených čísel $\mathbb{N}_0$ takto:

$$a \leq b \iff \text{existuje } r \in \mathbb{N}_0 \text{ splňující } b = a + r.$$

Tato definice nám umožňuje dokázat několik základních pravidel pro porovnávání přirozených čísel. Uvádíme je jako cvičení.

Cvičení 3. Ukaž, že pokud pro přirozená čísla a, b a c platí $a \leq b$ a $b \leq c$, potom $a \leq c$.

Cvičení 4. Ukaž, že pro všechna přirozená čísla n platí $n \leq n$.

Úloha 2. Ukaž, že pokud $a \leq b$ a současně $b \leq a$, pak nutně $a = b$.

V předchozích třech cvičeních a úloze jsme postupně ukázali tři vlastnosti porovnávání přirozených čísel, které definují *uspořádání*:

Definice. *Uspořádání* je relace R na nějaké množině, která je:

(1) *Tranzitivní*: pro všechna x, y, z z dané množiny platí: jestliže xRy a yRz, potom i xRz.
(2) *Reflexivní*: pro všechna x z dané množiny platí xRx neboli x je v relaci samo se sebou.
(3) *Antisymetrická*: pro všechna x, y z dané množiny platí „jestliže xRy a současně yRx, potom $x = y$“.

Tedy relace $\leq$ na přirozených číslech je relací uspořádání.

Navíc si všimněme dvou dalších zajímavých vlastností. Všechny prvky množiny přirozených čísel jsou vzájemně porovnatelné, to znamená, že pro každá dvě čísla a a b platí buď $a \leq b$, nebo $b \leq a$ (nebo obojí, viz vlastnost antisymetrie). Tuto vlastnost rozhodně nemají všechny množiny a relace: vezměme například relaci $\subset$ „být podmnožinou“.

Cvičení 5. Uvaž relaci „být podmnožinou“ $\subset$ na potenční množině $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ množiny $A = \{a, b\}$. Najdi dva prvky množiny $P(A)$, které mezi sebou nejsou porovnatelné, a dva prvky, které porovnatelné jsou.

Množina přirozených čísel je ještě k tomu takzvaně dobře uspořádaná, což znamená, že každá neprázdná podmnožina $\mathbb{N}_0$ má nejnižší prvek.

Definice. *Nejnižší prvek* je takový prvek x, že pro všechna y z dané množiny platí $x \leq y$.

Tvrzení. *Každá neprázdná podmnožina přirozených čísel má nejnižší prvek.*

Důkaz. Tvrzení dokážeme sporem. Pro spor předpokládejme, že $S \subset \mathbb{N}_0$ je neprázdná podmnožina, která nemá nejnižší prvek. Definujme $S^* = \{n \in \mathbb{N}_0;$ žádné z čísel $0, 1, \ldots, n$ není v $S\}$. Naším cílem bude ukázat, že $S^* = \mathbb{N}_0$, tedy že S je prázdná množina, což je spor.

Nejprve si všimněme, že $0 \in S^*$, neboť jinak by 0 byla v S a pak by S měla nejnižší prvek.

Nyní pokud $n \in S^*$, tak žádné z čísel $0, 1, \ldots, n$ není v S, a proto ani $n + 1$ nemůže být v S, jinak by $n + 1$ bylo nejnižším prvkem S. Tedy žádné z čísel od nuly po $n + 1$ není v S, a proto $(n + 1) \in S^*$.

Dle třetího Peanova axiomu máme $S^* = \mathbb{N}_0$, což je kýžený spor. □

Cvičení 6. Rozhodni a zdůvodni, zdali jsou následující množiny dobře uspořádané:

(1) množina celých čísel $\mathbb{Z}$,
(2) množina kladných racionálních čísel $\mathbb{Q}^+$,
(3) potenční množina[4] $P(A)$ množiny $A = \{a, b, c\}$.

Úloha 3. Ukaž, že každá ostře klesající posloupnost $x_1, x_2, x_3, \ldots$ přirozených čísel musí být konečná.

Je množina přirozených čísel jen jedna?

Zatím jsme v našem povídání hovořili o jedné množině přirozených čísel, která je definovaná Peanovými axiomy. Všechny vlastnosti aritmetiky a uspořádání přirozených čísel jsme dokázali pouze na základě těchto axiomů. Ale co když existuje ještě jiná množina, která splňuje tři Peanovy axiomy, která se od té naší liší?

Předpokládejme, že taková množina existuje, a nazvěme ji $\mathbb{N}_0^*$ spolu s funkcí následník s^*, která splňuje tři Peanovy axiomy. Potom můžeme stejným způsobem jako dříve odvodit pravidla aritmetiky a uspořádání. Předpokládali bychom, že tato množina bude „v podstatě stejná“ jako $\mathbb{N}_0$, až na to, že její prvky se mohou jinak jmenovat, ale chovat se budou stejně. To, jak se daný objekt chová, je ale právě to, o co nám v matematice jde! Vůbec nám nezáleží na tom, co daný objekt *je*, často to ani zjistit nemůžeme.

Proto zavedeme důležitý pojem, a to *izomorfismus*. Říkáme, že dvě množiny jsou izomorfní, pokud můžeme prvky jedné množiny přejmenovat, abychom dostali druhou množinu s tím, že všechny aritmetické vlastnosti zůstanou zachovány. V našem případě navíc potřebujeme izomorfismus, který zachovává i uspořádání.

Nebudeme zde zabíhat do detailů, pouze zmíníme, že bijekce mezi $\mathbb{N}_0$ a $\mathbb{N}_0^*$ zachovává sčítání, násobení i uspořádání. (Tedy například u sčítání nezáleží na tom, zda nejdřív dvě čísla sečteme a potom daný součet zobrazíme tou bijekcí (přejmenujeme), nebo zda nejdřív dvě čísla zobrazíme (přejmenujeme) a poté tyto obrazy sečteme.) To vše lze dokázat indukcí.

To znamená, že pouhé tři Peanovy axiomy definují přirozená čísla jednoznačně!

[4]Potenční množina je množina všech podmnožin dané množiny.

Závěr

Gratulujeme Ti k přečtení druhého dílu seriálu! Tento díl byl daleko více technický a rigorózní než díl předchozí. My doufáme, že si každý přišel aspoň v jednom díle na své. Axiomatický přístup, který jste měli možnost zažít v tomto povídání, je typický pro studium čisté matematiky na vysoké škole. Pokud Tě to zaujalo a chceš si o systémech čísel přečíst víc, vřele doporučujeme publikaci *The Foundations of Mathematics* (I. Stewart a D. Tall), ze které jsme jako autoři také čerpali.

Přejeme Ti hodně zdaru při řešení soutěžních úloh a těšíme se na Tebe u příštího dílu, tentokrát o algoritmech.

Návody ke cvičením

1. Podívej se na to, kolika způsoby lze spárovat prvky A s prvky B. Pozor na to, že musíš použít všechny prvky A právě jednou, ale prvky B se klidně můžou opakovat.

3. Rozepiš definice.

4. Použij $r = 0 \in \mathbb{N}_0$.

5. O $\{a\}$ a $\{b\}$ se nedá říct ani $\{a\} \subset \{b\}$, ani $\{b\} \subset \{a\}$. Naopak prvky $\emptyset$ a $\{a, b\}$ porovnatelné jsou, neboť $\emptyset \subset \{a, b\}$.

6. (1) Ne. (2) Ne. (3) Ne.

Návody k úlohám

2. Ukaž nejprve implikaci „jestliže $a + t = b + t$, pak $a = b$“.

3. Uvaž nejnižší prvek množiny $\{x_1, x_2, x_3, \dots\} \subset \mathbb{N}_0$. Pokračuj sporem.