1
MATEMATICKÝ TEXT

ukážka matematického textu

- T. Šalát et al.: *Algebra a teoretická aritmetika (2)*, Alfa, 1986, s. 20–21

Bez ťažkostí sa môžeme presvedčiť, že A_1^+ a A_2^+ spĺňajú podmienky lemy 1.2.2. (Urobte to!) Zrejme $A_1^+ \neq A_2^+$. Na základe vety 1.2.4 vidíme, že okruh $\mathsf{Z}[x]$ sa dá usporiadať dvoma rozličnými spôsobmi. Usporiadanie s pozitívnymi prvkami A_1^+ voláme *lexikografickým* a to druhé *antilexikografickým*.

Skôr ako sa budeme podrobnejšie zaoberať usporiadanými obormi integrity, zavedieme ďalší pojem.

Definícia 1.2.4. Zobrazenie $f\colon A_1 \to A_2$ medzi usporiadanými okruhmi $(A_1;\ +,\ \cdot,\ <)$ a $(A_2;\ +,\ \cdot,\ <)$ voláme *homomorfizmom*, ak f je izotónnym okruhovým homomorfizmom, t. j. pre všetky $x, y \in A_1$ platia podmienky (2) a (3):

$$f(x+y)=f(x)+f(y) \quad \text{a} \quad f(xy)=f(x)\,.\,f(y) \tag{2}$$

$$x<y \quad \text{implikuje} \quad f(x)<f(y) \tag{3}$$

Ak f je naviac prosté zobrazenie, tak f nazývame *vnorením* A_1 do A_2. Usporiadané okruhy A_1 a A_2 voláme *izomorfnými*, ak existuje izomorfné zobrazenie medzi A_1 a A_2, t. j. f je bijektívny homomorfizmus.

Veta 1.2.5. Nech $(A;\ +,\ \cdot,\ <)$ je usporiadaný obor integrity. Nech e je jednotkový prvok v A. Potom zobrazenie

$$\eta\colon n \mapsto ne \tag{4}$$

je vnorením usporiadaného oboru integrity celých čísel Z (s obvyklým usporiadaním) do daného usporiadaného oboru integrity A.

Dôkaz: Pripomeňme si, že ak n je celé číslo, tak ne je prvok, ktorý bol definovaný (v súlade s definíciou mocniny prvku grupy s multiplikatívnym zápisom) takto:

a) pre prirodzené číslo n indukciou:

$$1e=e, \quad (n+1)e=ne+1e,$$

b) pre $n=0$ rovnosťou $0e=0$,

c) pre záporné celé číslo n rovnosťou $ne=-(-n)e$.

Dokážte, že η je okruhový homomorfizmus, t. j. $(n+m)e=ne+me$ a $(nm)e= =(ne)(me)$ pre každé $n, m \in \mathsf{Z}$ (robili sme to už v prvom diele tejto knihy). Tvrdíme, že η je prosté zobrazenie. Teraz stačí už len ukázať, že $\operatorname{Ker}\eta=\{0\}$ (prečo?). Predpokladajme, že by existovalo $0 \neq n \in \operatorname{Ker}\eta$. Pretože $\operatorname{Ker}\eta$ je ideálom okruhu Z, tak aj $-n \in \operatorname{Ker}\eta$. Z toho vidíme, že môžeme dokonca predpokladať $n>0$. Lenže $n \in \operatorname{Ker}\eta$ znamená $ne=0$, čo je v spore s charakteristikou 0 okruhu A (veta 1.2.2). Teda $\operatorname{Ker}\eta=\{0\}$ a η je prosté zobrazenie. Ostáva ešte dokázať, že η je izotónnym zobrazením. Vezmime celé čísla $n<m$, t. j. $m-n>0$. Ale $me-ne=(m-n)e$, lebo η je okruhový homomorfizmus. Pretože $e>0$

a $m-n$ je prirodzené číslo, tak

$$0<e<e+e=2e<\ldots<(m-n)e=e+\ldots+e\ ((m-n)\text{-krát})$$

Vidíme, že $me-ne>0$, čo implikuje $ne<me$ v A a η je izotónnym zobrazením. Záverom sme dokázali, že η je vnorením. □

Dôsledok. Obor integrity celých čísel Z sa dá usporiadať len jediným spôsobom.

Dôkaz: Predpokladajme, že $\sqsubset$ je reláciou usporiadania na Z tak, že $(\mathsf{Z};\ +,\ \cdot,\ \sqsubset)$ tvorí usporiadaný obor integrity. Podľa predchádzajúcej vety máme vnorenie

$$\eta\colon n \mapsto ne = n1 = n$$

$(\mathsf{Z};\ +,\ \cdot,\ <)$ do $(\mathsf{Z};\ +,\ \cdot,\ \sqsubset)$. Pretože η je identické zobrazenie, $n<m$ implikuje $n \sqsubset m$ (lema 1.1.1). Obrátene, majme $r \sqsubset s$. Zrejme $r \neq s$. Potom alebo $s<r$, alebo $r<s$ z trichotómie usporiadania $<$. Lenže $s<r$ by znamenalo $s \sqsubset r$, čo by bol spor s $r \sqsubset s$. Ostáva len $r<s$. Teda relácia $\sqsubset$ sa rovná relácii $<$. □

Na opis usporiadaných oborov integrity Z a Q budeme potrebovať ďalšie dôležité pojmy.

Definícia 1.2.5. Hovoríme, že usporiadaný okruh $(A;\ +,\ \cdot,\ <)$ je *archimedovsky usporiadaný*, ak ku každým dvom prvkom $0<a<b$, $a, b \in A$, existuje také prirodzené číslo n, že $b<na$.

Definícia 1.3.6. Aspoň dvojprvková usporiadaná množina $(T;\ <)$ sa nazýva *husto usporiadaná*, ak $x, y \in T$ a $x<y$ implikuje existenciu $z \in T$ s vlastnosťou $x<z<y$.

Lema 1.2.3. Nech usporiadané okruhy $(A_1;\ +,\ \cdot,\ <)$ a $(A_2;\ +,\ \cdot,\ <)$ sú izomorfné. Ak je z nich archimedovsky usporiadaný jeden, druhý je tiež.

Dôkaz: Nech $f\colon A_1 \to A_2$ je izomorfizmus usporiadaných okruhov. Predpokladajme, že A_1 je archimedovsky usporiadaný. (Ak by bol taký A_2, úvahu urobíme pre $f^{-1}\colon A_2 \to A_1$.) Majme $0<a<b$ v A_2. Potom existujú $0<x<y$ v A_1 tak, že $f(x)=a$, $f(y)=b$. Podľa predpokladu máme $n \in \mathsf{N}$ s vlastnosťou $y<nx$. Pretože f je izomorfizmus, tak $na=nf(x)=f(nx)>f(y)=b$ a A_2 je tiež archimedovsky usporiadaný. □

Veta 1.2.6. Usporiadané obory integrity Z a Q s obvyklými usporiadaniami sú archimedovsky usporiadané. Q je husto usporiadané.

Dôkaz: Zrejme $1 \leqq n<m$ implikuje $m<(m+1)n$ v okruhu Z. Teda Z je archimedovsky usporiadaný obor integrity. Predpokladajme, že racionálne čísla $\frac{p}{q}$ a $\frac{r}{s}$ máme napísané vo vykrátenom tvare. Nech $0<\frac{p}{q}<\frac{r}{s}$ v usporiadanom obore integrity Q. Na základe príkladu 1.1.1 je to ekvivalentné s $0<ps<qr$ v Z. Pre Z

špecifiká matematického textu

- **lineárny** charakter
- odseky s rôznymi názvami
  - **definícia** (**označenie**)
  - **veta** (**lema**, **dôsledok**)
  - **dôkaz**
  - (ilustračný) **príklad**
  - poznámka, komentár
- matematická **symbolika**

matematická symbolika

- **premenné**
  - $x, y, n, k, A, B, V, \alpha, \beta, \varphi, \psi, \pi, \rho, \ldots$
  - odkazy na niektoré objekty
  - latinské a grécke písmená **v kurzíve**
- **špeciálne symboly**
  - $0, 1, 2{,}5, -4, \frac{3}{4}, \mathrm{\pi}, \mathrm{e}, \mathrm{i}, \mathbb{N}, \mathbb{Z}, \mathbb{R}, \sin, \lim_{x \to \ldots}, \in, \ldots$
  - značky konkrétnych objektov, funkcií a relácií
  - ak sú to zhluky písmen, tak **nie kurzívou**
- **logické symboly**
  - $=$, logické spojky ($\neg, \wedge, \vee, \ldots$), kvantifikátory ($\forall_x, \exists_x$)
- **zátvorky**
  - $(\ a\ ), [\ a\ ], \{\ a\ \}, \langle\ a\ \rangle$, ale aj napr. $(\ a\ ]$
  - každý druh zátvoriek má svoj špecifický význam

definícia

- napríklad:

> Nech n a d sú prirodzené čísla. Hovoríme, že *n je deliteľné d*, ak existuje prirodzené číslo také, že n je jeho d-násobkom.

- zavedenie **nového**, doteraz neexistujúceho **pojmu** pomocou už známych pojmov
- pre **každý** objekt (alebo ticu objektov) musí byť **jasné**, či sa ho definícia týka, alebo nie
- význam: **štrukturácia existujúceho poznania**
- používané vyjadrenia: „Hovoríme, že“, „nazývame“, „sa nazýva“, „bude“, ...
- žiadna premenná sa nesmie vyskytnúť práve raz

štruktúra definície

- **preambula**:

Nech (...).

  - vovedenie do kontextu
  - **deklarácia** použitých **premenných**

- **označenie definovaného pojmu**:

Hovoríme, že (...),

  - oficiálne **prvýkrát** sa objavuje nový pojem
    (a to včítane umiestnenia prípadných parametrov)
  - obvykle je graficky **zvýraznený**
    (ak má textový charakter, tak napríklad kurzívou)

- **popis vymedzujúcej situácie**:

ak (...).

  - všetky používané pojmy sú už **známe predtým**
  - definícia sa týka danej tice objektov **práve vtedy**,
    keď je pre jej objekty popísaná situácia splnená

príklad definície

- Nech n a d sú prirodzené čísla. Hovoríme, že *n je deliteľné d*, ak existuje prirodzené číslo také, že n je jeho d-násobkom.
  - preambula:

    Nech n a d sú prirodzené čísla.
  - označenie definovaného pojmu:

    Hovoríme, že *n je deliteľné d*,
  - popis vymedzujúcej situácie:

    ak existuje prirodzené číslo také, že n je jeho d-násobkom.
    - pre $n = 6$ a $d = 2$ situácia **nastáva**
      (vhodné prirodzené číslo existuje (je to 3)),
      takže **je pravda**, že 6 je deliteľné 2
    - pre $n = 5$ a $d = 2$ situácia **nenastáva**
      (žiadne vhodné prirodzené číslo neexistuje),
      takže **nie je pravda**, že 5 je deliteľné 2

korektnosť definície

- definícia (vymysleného) pojmu *dobrota*:

Nech n a k sú prirodzené čísla. Hovoríme, že *n je dobré*, ak k je deliteľné n.

- je číslo 4 dobré?
  - ak $n = 4$ a $k = 8$, tak k je deliteľné n,
    čiže číslo 4 **je** dobré
  - ak $n = 4$ a $k = 9$, tak k nie je deliteľné n,
    čiže číslo 4 **nie je** dobré
- táto „definícia“ je nekorektná!

veta

- príklad:

Nech n je prirodzené číslo. Potom ak n je deliteľné 4, tak n je deliteľné 2.

- **nový vzťah** už existujúcich pojmov
- nevzniká žiadny nový pojem
- význam: **nové poznanie**
- žiadna premenná sa nesmie vyskytnúť práve raz
- dôležité vety majú **meno**:
  - podľa autora (napríklad *Pytagorova veta*)
  - podľa obsahu (napríklad *veta o pevnom bode*)
- veta **musí mať dôkaz**
- **špeciálne typy viet** (podľa významu či rozsahu dôkazu)
  - **pozorovanie**
  - **lema**
  - **dôsledok**

štruktúra vety

- **preambula**:

  Nech (...).

  - vovedenie do kontextu
  - **deklarácia** použitých **premenných**

- **tvrdenie**:

  Potom (...).

  - **vyjadrenie vzťahu** (hodnôt) deklarovaných premenných
  - často má formu **implikácie** („ak (...), tak (...)“)

príklad vety

- $\boxed{\text{Nech } n \text{ je prirodzené číslo. Potom ak } n \text{ je deliteľné 4, tak } n \text{ je deliteľné 2.}}$
  - preambula:

    $\boxed{\text{Nech } n \text{ je prirodzené číslo.}}$
  - tvrdenie:

    $\boxed{\text{Potom ak } n \text{ je deliteľné 4, tak } n \text{ je deliteľné 2.}}$
    - tvrdenie má formu implikácie:
      - **predpoklad**:

        $\boxed{n \text{ je deliteľné } 4}$
      - **záver**:

        $\boxed{n \text{ je deliteľné } 2}$
  - pre $n = 8$ **predpoklad platí**,
    takže podľa vety musí platiť (a naozaj aj **platí**) jeho **záver**
  - pre $n = 9$ alebo $n = 10$ **predpoklad neplatí**,
    takže celé tvrdenie je triviálne **pravdivé**,
    a to **bez ohľadu na platnosť jeho záveru**

dôkaz

- veta:

  Nech n je prirodzené číslo. Potom ak n je deliteľné 4, tak n je deliteľné 2.

- dôkaz:

  Keďže predpokladáme, že n je deliteľné 4, existuje prirodzené číslo také, že n je jeho 4-násobkom. Ak toto číslo označíme k, tak n je 4-násobkom k, čiže $n = 4k$. Označme m prirodzené číslo $2k$, t. j. $2k = m$. Potom platí $4k = 2m$, čiže $n = 2m$. Existuje teda prirodzené číslo také, že n je jeho 2-násobkom, z čoho vyplýva, že n je deliteľné 2.

- význam: **zdôvodnenie platnosti vety**
- neoddeliteľná súčasť vety

dôkaz

- sled **racionálnych argumentov** rôznych typov:
  - **prepis** pojmu na iné pojmy **podľa** svojej **definície**
  - **odvolávka na predpoklad** vety
  - **odvolávka na iné** už skôr vyslovené (a dokázané) **tvrdenie**, ktoré sa nachádza v tomto texte (pravdaže, pred touto vetou)
  - **odvolávka na „autoritu“**, teda na všeobecne akceptované tvrdenie
  - čisto **logický dôsledok** už vyslovených argumentov
- posledný člen dôkazu je samotné tvrdenie vety
- používanie slov typu „keďže“, „pretože“, „lebo“, „teda“, „t. j.“, „takže“, „čiže“, „potom“, „preto“, „z čoho (vyplýva)“, „z toho (vyplýva)“, ...
- v dôkaze môžeme zaviesť **nové označenie** (zatiaľ nepoužitú premennú), jeho platnosť sa však po jeho skončení dôkazu končí tiež
- žiadna premenná sa nesmie v rámci vety a jej dôkazu vyskytnúť práve raz

príklad dôkazu

- sled argumentov:

  - $\boxed{\text{keďže predpokladáme, že } n \text{ je deliteľné } 4}$

    odvolávka na predpoklad vety

  - $\boxed{\text{existuje prirodzené číslo také, že } n \text{ je jeho } 4\text{-násobkom}}$

    prepis pojmu *byť deliteľný* na iné pojmy podľa svojej definície

  - $\boxed{\text{ak toto číslo označíme } k\text{, tak } n \text{ je } 4\text{-násobkom } k}$

    označenie (ľubovoľného) vyhovujúceho čísla
    zatiaľ nepoužitou premennou

  - $\boxed{\text{čiže } n = 4k}$

    prepis pojmu *-násobok* na iné pojmy podľa svojej definície

  - $\boxed{\text{označme } m \text{ prirodzené číslo } 2k\text{, t. j. } 2k = m}$

    označenie jediného vyhovujúceho čísla
    zatiaľ nepoužitou premennou

príklad dôkazu

- sled argumentov (pokračovanie):
  - $\boxed{\text{potom platí } 4k = 2m}$

    logický dôsledok
    (predchádzajúci vzťah sme vynásobili 2)
  - $\boxed{\text{čiže } n = 2m}$

    logický dôsledok
    (predchádzajúcich vzťahov $n = 4k$ a $4k = 2m$)
  - $\boxed{\text{existuje teda prirodzené číslo také, že } n \text{ je jeho 2-násobkom}}$

    logický dôsledok
    (je to číslo m)
  - $\boxed{\text{z čoho vyplýva, že } n \text{ je deliteľné 2}}$

    prepis pojmu *byť deliteľný* na iné pojmy podľa svojej definície

nepriame dôkazy

- namiesto vety dokazujeme **inú vetu**, z ktorej pôvodná vyplýva
- špeciálne **typy nepriamych dôkazov**:
  - obmenou
  - sporom
  - matematickou indukciou

dôkaz obmenou

- namiesto vety

  Ak platí A, tak platí B.

  sa dokazuje jej **obmena**, t. j. s ňou ekvivalentná veta

  Ak neplatí B, tak neplatí A.

príklad dôkazu obmenou

- veta:

  Ak prirodzené číslo nie je deliteľné 4, nie je deliteľné ani 8.

- priamy dôkaz:

  Ak prirodzené číslo n nie je deliteľné 4, tak platí jedna z týchto možností:

  - Platí $n = 4k + 1$ pre nejaké prirodzené číslo k.
    Pre číslo k máme dve možnosti:
    - Ak je k párne, tak $k = 2m$ pre nejaké prirodzené číslo m. Potom platí $n = 4k + 1 = 4(2m) + 1 = 8m + 1$, teda n nie je deliteľné 8.
    - Ak je k nepárne, tak $k = 2m+1$ pre nejaké prirodzené číslo m. Potom platí $n = 4k+1 = 4(2m+1)+1 = 8m+5$, teda n nie je deliteľné 8.
  - Platí $n = 4k + 2$ pre nejaké prirodzené číslo k.
    Pre číslo k máme dve možnosti:
    - Ak je k párne, tak $k = 2m$ pre nejaké prirodzené číslo m. Potom platí $n = 4k + 2 = 4(2m) + 2 = 8m + 2$, teda n nie je deliteľné 8.
    - Ak je k nepárne, tak $k = 2m+1$ pre nejaké prirodzené číslo m. Potom platí $n = 4k+2 = 4(2m+1)+2 = 8m+6$, teda n nie je deliteľné 8.
  - Platí $n = 4k + 3$ pre nejaké prirodzené číslo k.
    Pre číslo k máme dve možnosti:
    - Ak je k párne, tak $k = 2m$ pre nejaké prirodzené číslo m. Potom platí $n = 4k + 3 = 4(2m) + 3 = 8m + 3$, teda n nie je deliteľné 8.
    - Ak je k nepárne, tak $k = 2m+1$ pre nejaké prirodzené číslo m. Potom platí $n = 4k+3 = 4(2m+1)+3 = 8m+7$, teda n nie je deliteľné 8.

príklad dôkazu obmenou

- obmena vety:

  Ak prirodzené číslo je deliteľné 8, je deliteľné aj 4.

- dôkaz obmeny:

  Ak je prirodzené číslo n je deliteľné 8, má tvar $n = 8k$ pre nejaké prirodzené číslo k. Potom však platí $n = 4(2k)$, a teda n je deliteľné aj 4.

dôkaz sporom

- namiesto vety

  Ak platí A, tak platí B.

  sa dokazuje iná s ňou ekvivalentná veta

  Nemôže zároveň platiť A a neplatiť B.

- namiesto vety

  Platí B.

  sa dokazuje iná s ňou ekvivalentná veta

  Nemôže neplatiť B.

príklad dôkazu sporom

- veta:

$\sqrt{2}$ je iracionálne číslo.

- veta nemá predpoklad
- ekvivalentná reformulácia:

Nemôže neplatiť, že $\sqrt{2}$ je iracionálne číslo.

- dôkaz:

Predpokladajme, že $\sqrt{2}$ je, naopak, racionálne číslo. Existujú teda nesúdeliteľné celé čísla a a b také, že $\sqrt{2} = \frac{a}{b}$ a $b > 0$. Po umocnení dostávame $2 = \frac{a^2}{b^2}$, po vynásobení b^2 zasa $2b^2 = a^2$. Číslo a^2 je teda párne, takže musí byť párne aj a. Existuje teda celé číslo c také, že $a = 2c$. Po dosadení dostávame $2b^2 = (2c)^2$, z čoho po vydelení dvoma $b^2 = 2c^2$. Číslo b^2 je teda párne, takže musí byť párne aj b. To je však spor, lebo čísla a a b majú byť nesúdeliteľné.

dôkaz matematickou indukciou

- namiesto vety

  $\boxed{\text{Pre každé prirodzené číslo } n \text{ platí tvrdenie } T_n.}$

  stačí dokázať dve (často jednoduchšie) vety:

  1° $\boxed{\text{Platí tvrdenie } T_0.}$

  2° $\boxed{\text{Pre každé prirodzené číslo } k \text{ z platnosti tvrdenia } T_k \text{ vyplýva platnosť tvrdenia } T_{k+1}.}$

- špeciálne názvy:
  - 1° nazývame **1. indukčný krok**
  - 2° nazývame **2. indukčný krok**
  - T_k nazývame **indukčný predpoklad**

príklad dôkazu matematickou indukciou

- veta:

> Pre každé prirodzené číslo n platí
> $$0^2 + 1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1).$$

- označme T_n tvrdenie $0^2 + 1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$
- stačí dokázať dve omnoho jednoduchšie vety:

1° T_0, t. j.

> $0^2 = \frac{1}{6} \cdot 0 \cdot (0+1) \cdot (2 \cdot 0 + 1).$

2° Pre každé prirodzené číslo k z T_k vyplýva T_{k+1}, t. j.

> Pre každé prirodzené číslo k z platnosti
> $$0^2 + 1^2 + 2^2 + \cdots + k^2 = \frac{1}{6}k(k+1)(2k+1)$$
> vyplýva platnosť
> $$0^2 + 1^2 + 2^2 + \cdots + (k+1)^2 = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1).$$

príklad dôkazu matematickou indukciou

- dôkaz 1°:

Obe strany rovnosti sú rovné 0, tá preto platí.

- dôkaz 2°:

$$
\begin{aligned}
&0^2 + 1^2 + 2^2 + \cdots + (k+1)^2 \\
&= (0^2 + 1^2 + 2^2 + \cdots + k^2) + (k+1)^2, \\
&= \tfrac{1}{6} k(k+1)(2k+1) + (k+1)^2 \\
&\qquad \text{(podľa indukčného predpokladu)}, \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)), \\
&= \tfrac{1}{6}(k+1)(2k^2 + 7k + 6), \\
&= \tfrac{1}{6}(k+1)(k+2)(2k+3), \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1).
\end{aligned}
$$