Reálná a komplexní čísla

7. Těleso reálných čísel

7.1. Definice. Buď $(R, \leq)$ lineárně uspořádaná množina. Dvojice $\alpha = (A, B)$, kde $A \subseteq R$, $B \subseteq R$, se nazývá *řez v množině* R, jestliže platí:
(1) $A \cup B = R$, $A \neq \emptyset \neq B$,
(2) $x \in A$, $y \in B \Longrightarrow x < y$.
Je zřejmé, že množiny A, B jsou disjunktní, tedy systém $\{A, B\}$ tvoří rozklad na množině R.

Množina A se nazývá *dolní skupina řezu* α, množina B se nazývá *horní skupina řezu* α.

Jestliže dolní skupina řezu α má největší prvek a horní skupina řezu α má nejmenší prvek, pak řez α nazýváme *skok v množině* R. Jestliže dolní skupina řezu α nemá největší prvek a horní skupina řezu α nemá nejmenší prvek, pak řez α nazýváme *mezera v množině* R.

Mezi pojmem *hustě uspořádaná množina* a pojmem *skok* platí následující vztah.

7.2. Tvrzení. *Lineárně uspořádaná množina, která obsahuje alespoň dva prvky, je hustě uspořádaná právě tehdy, když nemá skoky.*

7.3. Příklady.
a) Nechť m je celé číslo, $A = \{x \in \mathbb{Z} \mid x \leq m\}$, $B = \{x \in \mathbb{Z} \mid x \geq m+1\}$. Pak dvojice (A, B) je skok v množině $\mathbb{Z}$ celých čísel.

b) Nechť m je libovolné racionální číslo. Mějme dánu množinu $\mathbb{Q} - \{m\}$, na níž je definováno lineární uspořádání stejným způsobem jako na množině $\mathbb{Q}$. Pak řez $\alpha = (A, B)$, kde $A = \{x \in \mathbb{Q} \mid x < m\}$, $B = \{x \in \mathbb{Q} \mid x > m\}$, je mezerou v $\mathbb{Q} - \{m\}$.

c) Nechť n je pevně zvolené přirozené číslo $(n > 1)$, $\alpha \in \mathbb{Q}, \alpha > 0$ a zároveň nechť neexistuje racionální číslo ξ takové, že $\xi^n = \alpha$. Položme

$$\begin{aligned} A &= \{\xi \in \mathbb{Q} \mid \xi < 0\} \cup \{\xi \in \mathbb{Q} \mid \xi \geq 0, \xi^n < \alpha\}, \\ B &= \{\xi \in \mathbb{Q} \mid \xi > 0, \xi^n > \alpha\}. \end{aligned}$$

Ukážeme, že dvojice (A, B) je mezera v množině $\mathbb{Q}$ racionálních čísel.

Zřejmě $\emptyset \neq A \subseteq \mathbb{Q}$, $\emptyset \neq B \subseteq \mathbb{Q}$, $A \cup B = \mathbb{Q}$. Nechť $\xi \in A$, $\eta \in B$. Pak $\eta > 0$, $\eta^n > \alpha$. Jestliže $\xi < 0$, pak $\xi < \eta$. Jestliže $\xi \geq 0$, pak $\xi^n < \alpha < \eta^n$, odkud plyne $\xi < \eta$. Tedy (A, B) je řez v množině $\mathbb{Q}$.

Předpokládejme, že horní skupina B má nejmenší prvek β. Protože množina racionálních čísel je hustě uspořádaná, existuje racionální číslo ξ splňující následující tři podmínky:

$$0 < \xi < \beta, \qquad \xi < \frac{\beta^n - \alpha}{n\beta^{n-1}}, \qquad \xi < \beta\tbinom{n}{\nu}\left[\tbinom{n}{\nu+1}\right]^{-1}$$

pro každé sudé číslo ν $(2 \leq \nu < n)$. Z těchto podmínek plyne, že $n\beta^{n-1}\xi < \beta^n - \alpha$, nebo-li $\beta^n - n\beta^{n-1}\xi > \alpha$ a $\binom{n}{\nu}\beta - \binom{n}{\nu+1}\xi > 0$.

Pokud položíme $\gamma = \beta - \xi$, potom $0 < \gamma < \beta$ a

$$\gamma^n = \sum_{\nu=0}^{n} \tbinom{n}{\nu}(-1)^\nu \beta^{n-\nu}\xi^\nu = \beta^n - n\beta^{n-1}\xi + \sum \beta^{n-\nu-1}\xi^\nu\left[\tbinom{n}{\nu}\beta - \tbinom{n}{\nu+1}\xi\right] + \varepsilon,$$

kde sčítání probíhá všechna sudá ν taková, že $2 \leq \nu < n$, a kde $\varepsilon = 0$ pro n liché a $\varepsilon = \xi^n > 0$ pro n sudé. Odtud, vzhledem k podmínkám kladeným na číslo ξ, plyne $\gamma^n > \alpha$. Tudíž $\gamma \in B$, což je spor s předpokladem, že β je nejmenší prvek B. Množina B tedy nemá nejmenší prvek.

Předpokládejme, že množina A má největší prvek β. Rozlišme nyní dva případy.

Nejprve nechť platí $\beta = 0$. Je-li $\alpha > 1$, položíme $\gamma = 1$, je-li $\alpha \leq 1$, položíme $\gamma = \frac{\alpha}{2}$. V obou případech dostáváme, že $\gamma^n < \alpha$, a tudíž $\gamma \in A$, což je však spor s tím, že β je největší prvek A, neboť $\beta = 0 < \gamma$.

Nechť nyní platí $\beta > 0$. Označme

$$\omega = \min \left\{(\alpha - \beta^n)\left[\tbinom{n}{\nu}\beta^{n-\nu}n\right]^{-1} \;\middle|\; 1 \leq \nu \leq n\right\}.$$

Jistě platí $\omega > 0$. Je-li dokonce $\omega > 1$, položíme $\xi = 1$. Je-li naopak $\omega \leq 1$, klademe $\xi = \frac{\omega}{2}$. V obou případech dostáváme $\xi^\nu < \omega$ pro každé $1 \leq \nu \leq n$, tedy

$$\xi^\nu < \tfrac{(\alpha-\beta^n)}{n}\left[\tbinom{n}{\nu}\beta^{n-\nu}\right]^{-1}$$

pro všechna $1 \leq \nu \leq n$. To znamená, že pro všechna uvažovaná ν platí nerovnost $\binom{n}{\nu}\beta^{n-\nu}\xi^\nu < \frac{\alpha-\beta^n}{n}$.

Položme nyní $\gamma = \beta + \xi$. Potom platí $\gamma > \beta$ a

$$\gamma^n = \beta^n + \sum_{\nu=1}^{n} \tbinom{n}{\nu}\beta^{n-\nu}\xi^\nu < \beta^n + n \cdot \tfrac{\alpha-\beta^n}{n} = \alpha.$$

Odtud plyne $\gamma \in A$, což je spor s předpokladem, že β je největší prvek A. Množina A tedy nemá největší prvek, a (A, B) je tudíž mezera v $\mathbb{Q}$.

Nyní ukážeme, že každou lineárně uspořádanou množinu lze vnořit do lineárně uspořádané množiny, která nemá mezery. Za tím účelem si nejdříve definujme pojem *vnoření lineárně uspořádaných množin*.

7.4. Definice. Buďte $(R, \leq)$, $(S, \preceq)$ lineárně uspořádané množiny. Zobrazení f množiny R do S se nazývá *vnoření lineárně uspořádané množiny* $(R, \leq)$ *do lineárně uspořádané množiny* $(S, \preceq)$, jestliže platí:

(1) f je injekce,

(2) pro libovolné $x, y \in R$, $x \leq y$ platí, že $f(x) \preceq f(y)$.

Řekneme pak, že *lineárně uspořádanou množinu* $(R, \leq)$ *lze vnořit (resp. je vnořena) do lineárně uspořádané množiny* $(S, \preceq)$. Vnoření f se též často nazývá *izomorfismus vzhledem k uspořádání* nebo *pořádkový izomorfismus lineárně uspořádaných množin.*

Protože je $(R, \leq)$ uspořádáno lineárně, pro vnoření f také platí, že:

$$x, y \in R,\ f(x) \preceq f(y) \Longrightarrow x \leq y.$$

Uspořádání $\preceq$ na množině S se často označuje stejným symbolem jako uspořádání $\leq$ na množině R. Prvek $r \in R$ se obvykle identifikuje s prvkem $f(r)$. Při této identifikaci je pak množina R podmnožinou množiny S.

7.5. Věta. *Každou lineárně uspořádanou množinu lze vnořit do lineárně uspořádané množiny bez mezer.*

Důkaz. Nechť $(R, \leq)$ je lineárně uspořádaná množina. Pro $r \in R$ označme symbolem $(r]$ množinu $\{x \in R \mid x \leq r\}$.

Nechť S značí systém dvojic (A, B), $A \subseteq R$, $B \subseteq R$ a (A, B) je mezera v R nebo $A = (r]$, $B = R - (r]$ pro nějaké $r \in R$. Zřejmě (A, B) je řez v R s eventuální výjimkou případu, kdy R má největší prvek m a $A = (m] = R$, $B = \emptyset$.

Pro $\alpha = (A, B) \in S$, $\beta = (C, D) \in S$ položíme $\alpha \preceq \beta$, jestliže $A \subseteq C$, což je ekvivalentní s podmínkou $B \supseteq D$. Snadno lze ukázat, že relace $\preceq$ na S je lineární uspořádání.

Ukážeme sporem, že lineárně uspořádaná množina $(S, \preceq)$ nemá mezery. Předpokládejme proto, že $(\mathcal{A}, \mathcal{B})$ je mezera v S. Položme

$$\mathcal{A}^\star = \bigcup_{(X,Y) \in \mathcal{A}} X, \qquad \mathcal{B}^\star = \bigcup_{(X,Y) \in \mathcal{B}} Y.$$

Zřejmě pak $\mathcal{A}^\star, \mathcal{B}^\star \subseteq R$ a $\mathcal{A}^\star \neq \emptyset$. Kdyby $\mathcal{B}^\star = \emptyset$, pak by musela mít množina R největší prvek a muselo by platit $\mathcal{B} = \{(R, \emptyset)\}$, což není možné kvůli našemu předpokladu, že $(\mathcal{A}, \mathcal{B})$ je mezera v S. Je tedy i $\mathcal{B}^\star$ neprázdná.

Ukážeme, že dvojice $(\mathcal{A}^\star, \mathcal{B}^\star)$ je mezera v R.

Nechť $r \in R$ je libovolné. Označme $\varrho = ((r], R - (r]) \in S$. Pak $\varrho \in \mathcal{A}$ nebo $\varrho \in \mathcal{B}$. Z prvního případu ihned plyne $r \in \mathcal{A}^\star$. Protože $\mathcal{B}$ nemá nejmenší prvek, z druhého případu dostáváme $r \in \mathcal{B}^\star$. Je tedy $\mathcal{A}^\star \cup \mathcal{B}^\star = R$.

Nechť $a \in \mathcal{A}^\star$, $b \in \mathcal{B}^\star$. Pak existuje $(A, B) \in \mathcal{A}$, $(C, D) \in \mathcal{B}$ tak, že $a \in A$, $b \in D$. Jelikož $(A, B) \preceq (C, D)$, máme $B \supseteq D$, tudíž $b \in B$ a odtud dostáváme $a < b$.

Dvojice $(\mathcal{A}^\star, \mathcal{B}^\star)$ je tedy řez v R. Kdyby $(\mathcal{A}^\star, \mathcal{B}^\star)$ nebyla mezera, musel by existovat největší prvek x množiny $\mathcal{A}^\star$ nebo nejmenší prvek y množiny $\mathcal{B}^\star$.

V prvním případě by pak ovšem existovalo $\xi = (X, Y) \in \mathcal{A}$ tak, že $x \in X$, a toto ξ by muselo být největším prvkem množiny $\mathcal{A}$, což není možné, neboť předpokládáme, že $(\mathcal{A}, \mathcal{B})$ je mezera v S. Podobně ve druhém případě by pak existovalo $\eta = (X, Y) \in \mathcal{B}$ tak, že $y \in Y$, přičemž toto η by se stalo nejmenším prvkem množiny $\mathcal{B}$, což opět není možné ze stejného důvodu.

Ukázali jsme si, že $(\mathcal{A}^\star, \mathcal{B}^\star)$ je mezera v R. To ovšem znamená $(\mathcal{A}^\star, \mathcal{B}^\star) \in S$. Pak $(\mathcal{A}^\star, \mathcal{B}^\star) \in \mathcal{A}$ nebo $(\mathcal{A}^\star, \mathcal{B}^\star) \in \mathcal{B}$. V prvním případě je $(\mathcal{A}^\star, \mathcal{B}^\star)$ největší prvek množiny $\mathcal{A}$, neboť pro libovolné $(C, D) \in \mathcal{A}$ platí $C \subseteq \mathcal{A}^\star$ z definice $\mathcal{A}^\star$, a tedy $(C, D) \preceq (\mathcal{A}^\star, \mathcal{B}^\star)$. Jenže existence největšího prvku množiny $\mathcal{A}$ je ve sporu s naším předpokladem, že $(\mathcal{A}, \mathcal{B})$ je mezera v S. Podobně ve druhém případě je $(\mathcal{A}^\star, \mathcal{B}^\star)$ nejmenší prvek množiny $\mathcal{B}$, což je spor ze stejného důvodu.

Dokázali jsme, že $(S, \preceq)$ nemá mezery.

Pro $r \in R$ položme $\psi(r) = ((r], R - (r])$. Pak ψ je vnoření $(R, \leq)$ do $(S, \preceq)$ a věta je dokázána.

7.6. Definice. Lineárně uspořádaná množina $(S, \preceq)$ sestrojená v důkazu věty 7.5 se nazývá *normální obal lineárně uspořádané množiny* $(R, \leq)$. Zobrazení ψ se nazývá *kanonické vnoření lineárně uspořádané množiny* $(R, \leq)$ *do jejího normálního obalu.*

Ztotožníme-li prvky $r \in R$ s dvojicemi $((r], R - (r]) = \psi(r)$, můžeme říci, že normální obal lineárně uspořádané množiny $(R, \leq)$ se skládá z prvků množiny R a z mezer v množině R. V dalším textu budeme uspořádání na normálním obalu označovat stejným symbolem jako uspořádání na R, tj. $\leq$.

Normální obal lineárně uspořádané množiny je v následujícím smyslu jejím „nejmenším obalem“, který nemá mezery.

7.7. Věta. *Nechť* $(R, \leq)$ *je lineárně uspořádaná množina,* $(S, \leq)$ *její normální obal a* ψ *kanonické vnoření* $(R, \leq)$ *do* $(S, \leq)$. *Buď* $(T, \leq)$ *lineárně uspořádaná množina bez mezer a* f *vnoření* $(R, \leq)$ *do* $(T, \leq)$. *Pak existuje vnoření* $\widetilde{f}$ *množiny* $(S, \leq)$ *do* $(T, \leq)$ *takové, že* $\widetilde{f} \circ \psi = f$.

Můžeme pak říci, že diagram na obrázku 7 komutuje.

$$\begin{tikzcd} & (S,\leq) \arrow[dd, dashed, "\widetilde{f}"] \\ (R,\leq) \arrow[ur, "\psi"] \arrow[dr, "f"'] & \\ & (T,\leq) \end{tikzcd}$$

Obr. 7.

Důkaz. Nechť $\sigma = (A, B) \in S$. Jestliže $A = (r]$, $B = R - (r]$ pro nějaké $r \in R$, pak položíme $\tilde{f}(\sigma) = f(r)$.

Jestliže (A, B) je mezera v R, položme

$$\begin{aligned} A^* &= \{t \in T \mid \exists\, a \in A, t \leq f(a)\}, \\ B^* &= \{t \in T \mid \exists\, b \in B, t \geq f(b)\}. \end{aligned}$$

Ukážeme, že množina A^* nemá největší prvek. Skutečně, je-li $\alpha \in A^*$ největší prvek A^*, pak podle definice A^* musí existovat $a \in A$ tak, že $\alpha \leq f(a)$, současně však $f(a) \leq \alpha$, neboť $f(a) \in A^*$ a α je největší prvek A^*. Tedy $\alpha = f(a)$. Protože pro libovolný prvek $c \in A$ platí $f(c) \in A^*$, je $f(c) \leq \alpha = f(a)$, odkud $c \leq a$, a tedy a je největší prvek A. To je spor, neboť jsme předpokládali, že řez (A, B) je mezera v R.

Podobně lze ukázat, že B^* nemá nejmenší prvek. Jistě pro libovolné $\alpha \in A^*$, $\beta \in B^*$ platí $\alpha < \beta$. Protože v T nejsou mezery, není (A^*, B^*) řez, a tedy existuje $s \in T - (A^* \cup B^*)$. Položme $\tilde{f}(\sigma) = s$.

Je zřejmé, že $\tilde{f} \circ \psi = f$. Nechť $\sigma, \tau \in S$, $\sigma < \tau$. Pak $\sigma = (A, B)$, $\tau = (C, D)$, přičemž existuje $e \in B \cap C$. Z definice zobrazení $\tilde{f}$ plyne $\tilde{f}(\sigma) < f(e) \leq \tilde{f}(\tau)$, a tedy $\tilde{f}$ je vnoření. Zobrazení $\tilde{f}$ tedy splňuje podmínky věty.

7.8. Věta. *Nechť $(R, \leq)$ je lineárně uspořádaná množina, $(S, \leq)$ její normální obal a ψ kanonické vnoření $(R, \leq)$ do $(S, \leq)$. Pak platí:*

(a) *je-li (A, B) skok v R, a největší prvek A, b nejmenší prvek B, pak $(\mathcal{A}, \mathcal{B})$ je skokem v S, přičemž $\mathcal{A} = \{s \in S \mid s \leq \psi(a)\}$, $\mathcal{B} = \{s \in S \mid s \geq \psi(b)\}$,*

(b) *je-li $(\mathcal{A}, \mathcal{B})$ skok v S, pak existují $a, b \in R$ takové, že $\psi(a)$ je největší prvek $\mathcal{A}$ a $\psi(b)$ je nejmenší prvek $\mathcal{B}$; přitom platí, že (A, B) je skokem v R, kde $A = \{r \in R \mid r \leq a\}$, $B = \{r \in R \mid r \geq b\}$.*

Jinými slovy: skoky v S jsou právě „obrazy" skoků v R při kanonickém vnoření.

Důkaz. (a) Množina $\mathcal{A}$ má největší prvek $\psi(a)$ a $\mathcal{B}$ má největší prvek $\psi(b)$. Pokud $(\mathcal{A}, \mathcal{B})$ je řez v S, pak je $(\mathcal{A}, \mathcal{B})$ skok. Abychom ověřili, že $(\mathcal{A}, \mathcal{B})$ je řez v S, ukážeme sporem, že $\mathcal{A} \cup \mathcal{B} = S$. Předpokládejme tedy naopak, že existuje $s \in S$, $s \notin \mathcal{A} \cup \mathcal{B}$. Odtud dostáváme, že $\psi(a) < s < \psi(b)$. Pak $s = (C, D)$ je řez v R. Z $\psi(a) < s$ plyne, že $a \in C$, z $s < \psi(b)$ plyne, že $b \in D$. Protože (A, B) je řez v R, je $A \cup B = R$, a tedy neexistuje $x \in R$ splňující $a < x < b$. Je tedy $s = (C, D) = (A, B) = \psi(a)$, což je spor a $(\mathcal{A}, \mathcal{B})$ je skutečně řezem v S.

(b) Předpokládejme, že $(\mathcal{A}, \mathcal{B})$ je skok v S. Označme $\alpha = (X, R - X)$ největší prvek $\mathcal{A}$, $\beta = (Y, R - Y)$ nejmenší prvek $\mathcal{B}$. Protože $\alpha < \beta$, existuje $b \in Y$, $b \notin X$. Pak b je největší prvek Y, neboť v opačném případě by existovalo $c \in Y$, $b < c$, a tedy $\alpha < \psi(b) < \psi(c) \leq \beta$, což by byl spor s tím, že $(\mathcal{A}, \mathcal{B})$ je řez v S. Je tedy $\beta = \psi(b)$. Současně je b nejmenším prvkem množiny $R - X$: v opačném případě by existovalo $d \in R - X$, $d < b$, a tedy $\alpha < \psi(d) < \psi(b) = \beta$, což by byl opět spor. Pak ovšem α nemůže být mezerou v R, a proto existuje $a \in R$ tak, že $\alpha = \psi(a)$, tj. a je největším prvkem X. Označíme-li $A = \{r \in R \mid r \leq a\}$, $B = \{r \in R \mid r \geq b\}$, pak $\alpha = (A, B)$ je skok v R.

7.9. Důsledek. *Lineárně uspořádaná množina nemá skoky právě tehdy, když její normální obal nemá skoky.*

7.10. Definice. Normální obal lineárně uspořádané množiny $(\mathbb{Q}, \leq)$ racionálních čísel se nazývá *lineárně uspořádaná množina reálných čísel* a značí se $(\mathbb{R}, \leq)$. Prvek množiny $\mathbb{R}$ se nazývá *reálné číslo*.

Racionální číslo q se zpravidla ztotožňuje s reálným číslem $((q], \mathbb{Q} - (q])$, tedy $\mathbb{Q} \subseteq \mathbb{R}$. Můžeme říci, že reálné číslo je buď racionální číslo nebo mezera v lineárně uspořádané množině racionálních čísel $\mathbb{Q}$. Reálné číslo, které není racionální, se nazývá *iracionální číslo*. Tudíž iracionální číslo je mezera v $\mathbb{Q}$.

7.11. Definice. Lineárně uspořádaná množina $(R, \leq)$ se nazývá *spojitě uspořádaná*, jestliže nemá skoky ani mezery.

7.12. Věta.

(a) *Množina reálných čísel $(\mathbb{R}, \leq)$ je spojitě uspořádaná.*

(b) *Jestliže $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$, pak existuje $\gamma \in \mathbb{Q}$ tak, že $\alpha < \gamma < \beta$.*

(c) *Množina reálných čísel $\mathbb{R}$ je rovna množině řezů v množině racionálních čísel $\mathbb{Q}$, jejichž horní skupina nemá nejmenší prvek.*

Důkaz. Tvrzení (a) plyne ihned z vět 6.12, 7.2 a 7.9. Protože množina racionálních čísel nemá největší prvek, dostáváme z (a) ihned tvrzení (c).

Nechť $\alpha = (A, B) \in \mathbb{R}$, $\beta = (C, D) \in \mathbb{R}$, $\alpha < \beta$. Pak $B \supseteq D$, $B \neq D$, tudíž existuje $q \in B - D$. Jelikož B nemá nejmenší prvek, existuje $c \in B$, $c < q$. Pak $A \subseteq (c] \subseteq C$, $A \neq (c] \neq C$, tedy pro racionální číslo $\gamma = ((c], \mathbb{Q} - (c])$ platí: $\alpha < \gamma < \beta$.

Věta je tím dokázána.

7.13. Definice. Nechť $\alpha = (A, B)$, $\beta = (C, D)$ jsou reálná čísla. Pak položíme $\alpha + \beta = (\mathbb{Q} - (B + D), B + D)$. (Výrazem $X + Y$ pro $X \subseteq \mathbb{Q}$, $Y \subseteq \mathbb{Q}$ rozumíme množinu $\{x + y \mid x \in X, y \in Y\}$).

7.14. Tvrzení. *Pro reálná čísla α, β je $\alpha + \beta$ zase reálným číslem. Tudíž $+$ je operací na množině $\mathbb{R}$. Jestliže α, β jsou racionální čísla, je reálné číslo $\alpha + \beta$ rovno dříve definovanému racionálnímu číslu $\alpha + \beta$.*

Důkaz. Nechť $\alpha = (A, B)$, $\beta = (C, D)$, $X = \mathbb{Q} - (B + D)$, $Y = B + D$. Pak $X \subseteq \mathbb{Q}$, $Y \subseteq \mathbb{Q}$, $X \cup Y = \mathbb{Q}$, $Y \neq \emptyset$. Zvolme $a \in A$, $c \in C$. Pak $a < b$ pro každý prvek $b \in B$, $c < d$ pro každý prvek $d \in D$, tudíž $a + c < b + d$ pro každý prvek $b \in B$ a každý prvek $d \in D$. Odtud plyne, že $a + c \in \mathbb{Q} - (B + D)$, tedy $X \neq \emptyset$.

Buď $x \in X$, $y \in Y$. Pak existují $b \in B$, $d \in D$ takové, že $y = b + d$. Jelikož $x \notin B + D$, je $x - b \notin D$. Proto platí $x - b \in C$, z čehož plyne nerovnost $x - b < d$. Tedy $x < b + d = y$. Dvojice (X, Y) je pak řezem na $\mathbb{Q}$. Stačí ukázat, že Y nemá nejmenší prvek.

Nechť $y \in Y$. Pak existují $b \in B$, $d \in D$ taková, že $y = b + d$. Jelikož B a D nemají nejmenší prvek, existují $u \in B$, $v \in D$, $u < b$, $v < d$. Pak $w = u + v \in Y$,

$w < y$. Tedy Y nemá nejmenší prvek, tudíž $\alpha + \beta = (X, Y)$ je reálné číslo.

Druhý výrok tohoto tvrzení lze již dokázat snadno.

7.15. Lemma. *Nechť (A, B) je řez v $\mathbb{Q}$, $d \in \mathbb{Q}$, $d > 0$. Pak existují prvky $a \in A$, $b \in B$ takové, že a není největší prvek množiny A a platí $d = b - a$.*

Důkaz. Podle tvrzení 6.12 existuje $f \in \mathbb{Q}$, $0 < f < d$. Zvolme nyní $x \in A$, $y \in B$ tak, aby x nebylo největším prvkem množiny A. Podle tvrzení 6.14 existuje přirozené číslo n takové, že $\frac{y-x}{f} < n$. Tudíž $y < nf + x$, odkud plyne $nf + x \in B$.

Buď m nejmenší přirozené číslo s vlastností $x + mf \in B$. Pak $x + (m-1)f \in A$.

Jestliže $x + (m-1)f \in A$ je největší prvek množiny A, pak $m \geq 2$ a položíme $a = x + (m-2)f, b = x + (m-2)f + d = a + d$. Jestliže $x + (m-1)f$ není největší prvek množiny A, položíme $a = x + (m-1)f$, $b = x + (m-1)f + d = a + d$. Odtud plyne lemma.

7.16. Věta. *Grupoid $(\mathbb{R}, +)$ je komutativní grupa. Nulovým prvkem této grupy je racionální číslo $0 = ((0], \mathbb{Q} - (0])$. Pro $\alpha = (A, B) \in \mathbb{R}$ je opačným prvkem $-\alpha = (\mathbb{Q} - (-\widetilde{A}), -\widetilde{A})$, kde*

$$\widetilde{A} = \begin{cases} A, & \text{jestliže } A \text{ nemá největší prvek,} \\ A - \{m\}, & \text{jestliže } m \text{ je největší prvek množiny } A. \end{cases}$$

(Pro $X \subseteq \mathbb{Q}$ značí $-X$ množinu $\{-x \mid x \in X\}$.)

Důkaz. Zřejmě je operace $+$ na $\mathbb{R}$ komutativní a pro libovolné $X, Y, Z \subseteq \mathbb{Q}$ platí $(X + Y) + Z = X + (Y + Z)$, tudíž $(\mathbb{R}, +)$ je komutativní pologrupa.

Dokažme, že $((0], \mathbb{Q} - (0])$ je nulovým prvkem uvažované pologrupy. Nechť $\alpha = (A, B) \in \mathbb{R}$. Zřejmě $B + (\mathbb{Q} - (0]) \subseteq B$. Buď $b \in B$. Pak existuje $c \in B$, $c < b$. Položme $g = b - c$. Pak $g \in \mathbb{Q} - (0]$, a tudíž $b = c + g \in B + (\mathbb{Q} - (0])$. Odtud plyne $B + (\mathbb{Q} - (0]) = B$, a tedy $((0], \mathbb{Q} - (0])$ je nulovým prvkem pologrupy $(\mathbb{R}, +)$.

Položme $X = \mathbb{Q} - (-\widetilde{A})$, $Y = -\widetilde{A}$. Pak $X \subseteq \mathbb{Q}$, $Y \subseteq \mathbb{Q}$, $Y \neq \emptyset$, $X \cup Y = \mathbb{Q}$, $X \cap Y = \emptyset$, $-B \subseteq X$, tedy $X \neq \emptyset$. Buď $x \in X$, $y \in Y$. Pak existuje $a \in A$, které není největším prvkem množiny A, takové, že $y = -a$. Kdyby $y < x$, pak $x > -a$, tudíž $-x < a$, odkud plyne, že $-x \in \widetilde{A}$. Odtud dostáváme, že $x \in Y$, což je spor. Tedy (X, Y) je řez v $\mathbb{Q}$. Jelikož množina $\widetilde{A}$ nemá největší prvek, nemá množina Y nejmenší prvek, což znamená, že $\beta = (X, Y)$ je reálné číslo.

Zřejmě $B + Y \subseteq \mathbb{Q} - (0]$. Buď $d \in \mathbb{Q} - (0]$. Podle lemmatu 7.15 existují $a \in \widetilde{A}$, $b \in B$ tak, že $d = b - a$. Položíme-li $y = -a$, je $y \in Y$, $d = b + y$, tudíž $B + Y = \mathbb{Q} - (0]$, z čehož plyne, že $\alpha + \beta = 0$. Věta je tím dokázána.

7.17. Věta. *Nechť $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. Pak platí:*

(a) $\alpha < \beta \iff \alpha + \gamma < \beta + \gamma$,

(b) $\alpha \leq \beta \iff \alpha + \gamma \leq \beta + \gamma$,

(c) *jestliže $\alpha < \beta$, $\gamma < \delta$ nebo $\alpha \leq \beta$, $\gamma < \delta$ nebo $\alpha < \beta$, $\gamma \leq \delta$, potom $\alpha + \gamma < \beta + \delta$,*

(d) $\alpha \leq \beta$, $\gamma \leq \delta \Longrightarrow \alpha + \gamma \leq \beta + \delta$.

Důkaz. Nechť $\alpha = (A, B)$, $\beta = (C, D)$, $\gamma = (E, F)$ jsou reálná čísla. Dokažme nejprve výrok (a).

„$\Longrightarrow$“ Nechť $\alpha < \beta$. Pak $B \supseteq D$, $B \neq D$, tudíž $B + F \supseteq D + F$. Dokažme, že $B + F \neq D + F$.

Existují $b^*, b \in B$, $b < b^*$, $b^* \notin D$. Podle lemmatu 7.15 existují $f \in F$, $e \in E$ taková, že $b^* - b = f - e$. Položme $w = b + f$. Pak $w \in B + F$. Předpokládejme nyní, že $w \in D + F$, pak existují $x \in D, y \in F$ taková, že $w = x + y$. Pak $x + y = b + f = e + b^*$, $e < y$, tudíž $b^* > x$, z čehož plyne $b^* \in D$, což je spor. Tedy $w \notin D + F$ a $B + F \neq D + F$, a tudíž $\alpha + \gamma < \beta + \gamma$.

„$\Longleftarrow$“ Jestliže $\alpha + \gamma < \beta + \gamma$, pak podle předešlého platí $\alpha = \alpha + \gamma + (-\gamma) < \beta + \gamma + (-\gamma) = \beta$. Platí výrok (a).

Výroky (b), (c), (d) lze z výroku (a) snadno odvodit.

7.18. Definice. Nechť $\alpha = (A, B)$, $\beta = (C, D)$ jsou libovolná reálná čísla. Je-li $\alpha \geq 0$, $\beta \geq 0$, položíme

$$\alpha \cdot \beta = (\mathbb{Q} - B \cdot D, B \cdot D).$$

(Výraz $X \cdot Y$ značí pro $X \subseteq \mathbb{Q}$, $Y \subseteq \mathbb{Q}$ množinu $\{x \cdot y \mid x \in X, y \in Y\}$).

V ostatních případech definujeme součin $\alpha \cdot \beta$ následovně:

$$\alpha \cdot \beta = \begin{cases} -(-\alpha) \cdot \beta & \text{pro } \alpha < 0,\ \beta \geq 0, \\ -[\alpha \cdot (-\beta)] & \text{pro } \alpha \geq 0,\ \beta < 0, \\ (-\alpha) \cdot (-\beta) & \text{pro } \alpha < 0,\ \beta < 0. \end{cases}$$

7.19. Tvrzení. *Pro $\alpha, \beta \in \mathbb{R}$ je $\alpha \cdot \beta \in \mathbb{R}$. Tudíž $\cdot$ je operace na $\mathbb{R}$. Jestliže α, β jsou racionální čísla, pak reálné číslo $\alpha \cdot \beta$ je rovno dříve definovanému racionálnímu číslu $\alpha \cdot \beta$.*

Důkaz. Nechť $\alpha = (A, B)$, $\beta = (C, D) \in \mathbb{R}$. Předpokládejme nejdříve, že $\alpha \geq 0$, $\beta \geq 0$ a položme $X = \mathbb{Q} - B \cdot D$, $Y = B \cdot D$. Zřejmě $X \subseteq \mathbb{Q}$, $Y \subseteq \mathbb{Q}$, $X \cup Y = \mathbb{Q}$, $Y \neq \emptyset$, $Y \subseteq \{q \in \mathbb{Q} \mid q > 0\}$. Tudíž $X \supseteq (0]$, z čehož plyne $X \neq \emptyset$.

Nechť $x \in X$, $y \in Y$. Potom musí existovat $b \in B$, $d \in D$ taková, že $y = b \cdot d$ $(b > 0, d > 0)$. Předpokládejme, že $x > y$. Pak $\frac{x}{d} > b$, a tudíž $\frac{x}{d} \in B$, odkud plyne $x \in B \cdot D$, což je spor. Tedy $x < y$, což znamená, že $\alpha \cdot \beta = (X, Y)$ je řezem v $\mathbb{Q}$. Jelikož B, D nemají nejmenší prvek, podle 6.10 (e) nemá nejmenší prvek ani množina Y. Takže $\alpha \cdot \beta \in \mathbb{R}$.

Nechť nyní $\alpha, \beta \in \mathbb{Q}$. Pak $B = \{t \in \mathbb{Q} \mid t > \alpha\}$, $D = \{s \in \mathbb{Q} \mid s > \beta\}$. Abychom ukázali, že reálné číslo $\alpha \cdot \beta$ splyne s dříve definovaným racionálním číslem $\alpha \cdot \beta$, je třeba dokázat, že $\{t \cdot s \mid t \in B, s \in D\} = \{u \in \mathbb{Q} \mid u > \alpha \cdot \beta\}$, kde oba symboly $\cdot$ značí dříve definované násobení racionálních čísel. Jsou-li $t, s \in \mathbb{Q}$, $t > \alpha$, $s > \beta$, pak $t \cdot s > \alpha \cdot \beta$ podle věty 6.10 (e), neboť $\alpha \geq 0$ a $\beta \geq 0$. Tím jsme ověřili inkluzi „$\subseteq$“.

Nechť nyní $u \in \mathbb{Q}$, $u > \alpha \cdot \beta$. Ukažme, že existují $t, s \in \mathbb{Q}$, $t > \alpha$, $s > \beta$ tak, že $u = t \cdot s$. Je-li $\alpha = 0$, stačí volit $s = \beta + 1$, $t = \frac{u}{\beta+1}$. Předpokládejme dále, že $\alpha \neq 0$.

Zvolme $v \in \mathbb{Q}$ tak, aby $u > v > \alpha \cdot \beta$ (existence takového v je zaručena tvrzením
6.12). Položme $s = \frac{v}{\alpha}$, $t = \frac{u\alpha}{v}$. Podle 6.10 (e) z $v > \alpha \cdot \beta$ plyne $s > \beta$ a z $u > v$
plyne $t > \alpha$. Přitom jistě $t \cdot s = u$. Dokázali jsme inkluzi „$\supseteq$“, a tedy rovnost.
Ostatní případy, kdy α nebo β je záporné, odsud snadno vyplynou.

7.20. Věta. *Trojice $(\mathbb{R}, +, \cdot)$ je těleso. Jednotkovým prvkem tohoto tělesa je racionální číslo $1 = ((1], \mathbb{Q} - (1])$ a pro reálné číslo $\alpha = (A, B) > 0$ platí, že $\alpha^{-1} = (X, Y)$, kde*

$$Y = \{a^{-1} \mid a \in \widetilde{A}, a > 0\},$$

$$X = \mathbb{Q} - Y.$$

Pro $\alpha < 0$ platí: $\alpha^{-1} = -(-\alpha)^{-1}$.
(Symbol $\widetilde{A}$ má stejný význam jako v 7.16.)

Důkaz. Zřejmě je operace $\cdot$ komutativní. Nechť jsou nyní dána reálná čísla
$\alpha = (A, B)$, $\beta = (C, D)$, $\gamma = (E, F) \in \mathbb{R}$. Předpokládejme nejdříve, že jsou
nezáporná, tedy $\alpha \geq 0$, $\beta \geq 0$, $\gamma \geq 0$. Pak $\alpha \cdot \beta \geq 0$, $\beta \cdot \gamma \geq 0$ a platí

$$\begin{aligned} (\alpha \cdot \beta) \cdot \gamma &= (\mathbb{Q} - (B \cdot D) \cdot F, (B \cdot D) \cdot F), \\ \alpha \cdot (\beta \cdot \gamma) &= (\mathbb{Q} - B \cdot (D \cdot F), B \cdot (D \cdot F)). \end{aligned}$$

Jelikož $(B \cdot D) \cdot F = B \cdot (D \cdot F)$, je $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.
Pro ostatní případy se již tvrzení $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ snadno dokáže. Tudíž
$(\mathbb{R}, \cdot)$ je komutativní pologrupa.
Nechť $\alpha \geq 0$. Zřejmě $(\mathbb{Q} - (1]) \cdot B \subseteq B$. Nechť $b \in B$. Pak existuje $c \in B$,
takové, že $c < b$. Potom $x = \frac{b}{c} > 1$, a tudíž $x \in (\mathbb{Q} - (1])$, z čehož dostáváme
$b \in (\mathbb{Q} - (1]) \cdot B$. Tedy $1 \cdot \alpha = \alpha$. Pro $\alpha < 0$ je $1 \cdot \alpha = -(1 \cdot (-\alpha)) = -(-\alpha) = \alpha$.
Takže $1 = ((1], \mathbb{Q} - (1])$ je jednotkovým prvkem pologrupy $(\mathbb{R}, \cdot)$.
Dokažme nyní, že inverze ke kladnému reálnému α je opravdu reálným číslem.
Buď $\alpha = (A, B) > 0$, $Y = \{a^{-1} \mid a \in \widetilde{A}, a > 0\}$, $X = \mathbb{Q} - Y$. Zřejmě $\emptyset \neq X \subseteq \mathbb{Q}$,
$\emptyset \neq Y \subseteq \mathbb{Q}$, $X \cup Y = \mathbb{Q}$. Nechť $x \in X$, $y \in Y$. Pak existuje $a \in \widetilde{A}$, $a > 0$, $y = a^{-1}$.
Jestliže $x \leq 0$, pak $x < y$. Je-li $x > 0$, pak $x^{-1} \notin \widetilde{A}$, tudíž $x^{-1} > a$, z čehož plyne,
že $x < y$. Dvojice (X, Y) je tedy řezem v $\mathbb{Q}$. Jelikož množina $\widetilde{A}$ nemá největší
prvek, nemá množina Y nejmenší prvek. Tedy $\xi = (X, Y) \in \mathbb{R}$, přičemž zřejmě
$\xi > 0$.
Ukažme nyní, že $\xi = (X, Y)$ je skutečně inverzním prvkem k prvku α. Platí, že
$\alpha \cdot \xi = (\mathbb{Q} - B \cdot Y, B \cdot Y)$. Nechť $z \in B \cdot Y$. Pak existují $b \in B$, $a \in \widetilde{A}$, $a > 0$ tak, že
$z = b \cdot a^{-1}$. Platí, že $a < b$, tudíž $z = b \cdot a^{-1} > 1$, což znamená, že $B \cdot Y \subseteq \mathbb{Q} - (1]$.
Ukažme, že platí i opačná inkluze. Buď $z \in \mathbb{Q}, z > 1$. Pak $z = 1 + d$, kde
$d \in \mathbb{Q}$, $d > 0$. Zvolme $a \in \widetilde{A}$, $a > 0$, $b \in B$. Podle věty 6.14 existuje přirozené
číslo n takové, že $\frac{b-a}{da} < n$, tedy $\frac{b}{a} < 1 + dn \leq (1+d)^n$, a proto $b < az^n$. Je tedy
$az^n \in B$. Buď m nejmenší přirozené číslo s vlastností $az^m \in B$. Pak $az^{m-1} \notin B$,
a proto $az^{m-1} \in A$. Jestliže $az^{m-1} \in \widetilde{A}$, pak $(az^{m-1})^{-1} \in Y$, a tedy $z = (az^m) \cdot$
$\cdot (az^{m-1})^{-1} \in B \cdot Y$. Jestliže naopak $az^{m-1} \notin \widetilde{A}$, znamená to, že az^{m-1} je největší

prvek A a že $m > 1$. Protože $1 < 1 + \frac{d}{2} < 1 + d = z$, platí $az^{m-2}(1 + \frac{d}{2}) <$ $< az^{m-1} < az^{m-1}(1 + \frac{d}{2})$. Odtud $az^{m-2}(1 + \frac{d}{2}) \in \widetilde{A}$, $az^{m-1}(1 + \frac{d}{2}) \in B$. Opět tedy $z = (az^{m-1}(1 + \frac{d}{2})) \cdot (az^{m-2}(1 + \frac{d}{2}))^{-1} \in B \cdot Y$. Tím jsme ukázali, že platí $\mathbb{Q} - (1] \subseteq B \cdot Y$, což vzhledem k předchozímu znamená, že $\mathbb{Q} - (1] = B \cdot Y$. Odtud plyne $\alpha \cdot \xi = 1$ a $\xi = \alpha^{-1}$.

Pro $\alpha < 0$ existuje $\xi \in \mathbb{R}$, $\xi > 0$ takové, že $(-\alpha) \cdot \xi = 1$. Pro toto $\xi \in \mathbb{R}$ platí $\alpha \cdot (-\xi) = (-\alpha) \cdot [-(-\xi)] = (-\alpha) \cdot \xi = 1$, tudíž $-\xi = \alpha^{-1}$.

Zbývá dokázat platnost distributivního zákona. Pro $\alpha \geq 0$, $\beta \geq 0$, $\gamma \geq 0$ dostáváme

$$\begin{aligned} \alpha \cdot (\beta + \gamma) &= (\mathbb{Q} - B \cdot (D + F), B \cdot (D + F)), \\ \alpha \cdot \beta + \alpha \cdot \gamma &= (\mathbb{Q} - (B \cdot D + B \cdot F), (B \cdot D + B \cdot F)). \end{aligned}$$

Zřejmě $B \cdot (D + F) \subseteq B \cdot D + B \cdot F$. Nechť $q \in B \cdot D + B \cdot F$. Pak existují $u, v \in B$, $d \in D$, $f \in F$ taková, že $q = ud + vf$. Bez újmy na obecnosti můžeme předpokládat, že $u \leq v$. Pak $q = u(d + f) + (v - u)f \geq u(d + f) \in B \cdot (D + F)$, odkud $q \in B \cdot (D + F)$. Tedy $B \cdot (D + F) = B \cdot D + B \cdot F$ a dostáváme tak, že $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Pro ostatní případy lze odtud platnost distributivního zákona snadno dokázat. Např. pro $\alpha \geq 0$, $\beta \geq 0$, $\gamma < 0$, $\beta + \gamma \geq 0$ je

$$\alpha \cdot (\beta + \gamma) - \alpha \cdot \gamma = \alpha \cdot (\beta + \gamma) + \alpha \cdot (-\gamma) = \alpha \cdot [\beta + \gamma + (-\gamma)] = \alpha \cdot \beta.$$

Tudíž $(\mathbb{R}, +, \cdot)$ je komutativní okruh a vzhledem k výše dokázanému je i tělesem.

7.21. Definice. Těleso $(\mathbb{R}, +, \cdot)$ se nazývá *těleso reálných čísel* a často se označuje pouze symbolem $\mathbb{R}$. Tímto symbolem budeme též označovat celou čtveřici $(\mathbb{R}, +, \cdot, \leq)$, tudíž $\mathbb{R} = (\mathbb{R}, +, \cdot, \leq)$. Operace $\cdot$ se v běžném zápise často nevyznačuje, tedy pro $\alpha, \beta \in \mathbb{R}$ je $\alpha\beta = \alpha \cdot \beta$.

Následující tvrzení plyne z definice součinu reálných čísel a z věty 7.20.

7.22. Tvrzení. *Nechť $\alpha, \beta \in \mathbb{R}$. Pak platí:*
(a) $\alpha > 0 \Longrightarrow \alpha^{-1} > 0$,
(b) $\alpha < 0 \Longrightarrow \alpha^{-1} < 0$,
(c) $\alpha > 0, \beta > 0$ *nebo* $\alpha < 0, \beta < 0 \Longrightarrow \alpha \cdot \beta > 0$, $\frac{\alpha}{\beta} > 0$,
(d) $\alpha > 0, \beta < 0$ *nebo* $\alpha < 0, \beta > 0 \Longrightarrow \alpha \cdot \beta < 0$, $\frac{\alpha}{\beta} < 0$.

7.23. Věta. *Nechť $\alpha, \beta, \gamma \in \mathbb{R}$.*
(a) *pro $\gamma > 0$ platí:* $\alpha < \beta \Longleftrightarrow \alpha \cdot \gamma < \beta \cdot \gamma$, $\alpha \leq \beta \Longleftrightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$,
(b) *pro $\gamma < 0$ platí:* $\alpha < \beta \Longleftrightarrow \beta \cdot \gamma < \alpha \cdot \gamma$, $\alpha \leq \beta \Longleftrightarrow \beta \cdot \gamma \leq \alpha \cdot \gamma$.

Důkaz. Nechť $\alpha < \beta$, pak podle 7.17 je $\beta - \alpha > 0$, a tedy podle 7.22 platí $(\beta - \alpha)\gamma > 0$, tj. $\beta\gamma - \alpha\gamma > 0$. Opět podle 7.17 dostáváme $\alpha\gamma < \beta\gamma$.

Naopak v případě, že $\alpha \cdot \gamma < \beta \cdot \gamma$, dostaneme (jelikož podle 7.22 (a) je $\gamma^{-1} > 0$) $\alpha = (\alpha \cdot \gamma) \cdot \gamma^{-1} < (\beta \cdot \gamma) \cdot \gamma^{-1} = \beta$. Tím je platnost (a) dokázána.

Výrok (b) se dokáže analogicky.

8. Binomické rovnice a g-adický rozvoj v reálném oboru

8.1. Lemma. *Nechť $\alpha_1, \dots, \alpha_n$ jsou kladná reálná čísla. Nechť dále a je racionální číslo s vlastností $0 < a < \alpha_1 \cdot \ldots \cdot \alpha_n$. Pak existují racionální čísla $a_1, \dots, a_n$, splňující nerovnost $0 < a_i < \alpha_i$ pro každé $i \in \{1, \dots, n\}$, taková, že platí:*

$$a = a_1 \cdot \ldots \cdot a_n.$$

Důkaz. Nejprve důkaz provedeme pro případ $n = 2$. Podle 7.12 (b) existuje racionální číslo a_2 takové, že $\frac{a}{\alpha_1} < a_2 < \alpha_2$. Položíme-li $a_1 = \frac{a}{a_2}$, pak čísla a_1, a_2 vyhovují podmínkám lemmatu.

Pro obecné n dokážeme lemma indukcí: pro $n = 1$ je lemma zřejmé, pro $n = 2$ bylo dokázáno. Předpokládejme tedy, že $n > 2$ a že pro $n - 1$ lemma platí. Pak existují racionální čísla $a_1, a_2, \dots, a_{n-2}, b$ tak, že $0 < a_1 < \alpha_1$, $0 < a_2 < \alpha_2, \dots$, $0 < a_{n-2} < \alpha_{n-2}$, $0 < b < \alpha_{n-1}\alpha_n$, $a = a_1 \cdot \ldots \cdot a_{n-2} \cdot b$. Podle dokázaného případu $n = 2$ však existují racionální čísla a_{n-1}, a_n taková, že $0 < a_{n-1} < \alpha_{n-1}$, $0 < a_n < \alpha_n$, $b = a_{n-1} \cdot a_n$. Tudíž lemma platí pro libovolné přirozené n.

8.2. Věta. *Nechť n je přirozené číslo, α reálné číslo. Pak platí:*

(a) *Jestliže n je sudé a $\alpha \geq 0$, pak binomická rovnice $x^n = \alpha$ je řešitelná v $\mathbb{R}$. Jestliže ξ je řešením této rovnice, pak $\{\xi, -\xi\}$ je množinou všech řešení rovnice $x^n = \alpha$ v $\mathbb{R}$.*

(b) *Jestliže n je sudé a $\alpha < 0$, pak binomická rovnice $x^n = \alpha$ nemá v $\mathbb{R}$ řešení.*

(c) *Jestliže n je liché, pak binomická rovnice $x^n = \alpha$ má v $\mathbb{R}$ právě jedno řešení ξ. Navíc platí:*

$$\begin{aligned} \alpha > 0 &\implies \xi > 0, \\ \alpha = 0 &\implies \xi = 0, \\ \alpha < 0 &\implies \xi < 0. \end{aligned}$$

Důkaz. Nechť $\alpha > 0$. Položme $B = \{q \in \mathbb{Q} \mid q^n > \alpha, q > 0\}$, $A = \mathbb{Q} - B$, a dokažme, že (A, B) je řez v $\mathbb{Q}$. Ze 7.12 (b) plyne existence racionálního čísla q takového, že $\alpha + 1 < q < \alpha + 2$. Pak $q > 1$, a tedy $q^n \geq q > \alpha$. Proto $B \neq \emptyset$. Jelikož $0 \in A$, máme $A \neq \emptyset$. Jistě $A \cup B = \mathbb{Q}$. Nechť $a \in A, b \in B$. Je-li $a \leq 0$, pak zřejmě $a < b$. Předpokládejme, že $a > 0, a > b$. Pak $\alpha < b^n < a^n$, což však není možné. Tudíž $a < b$ a (A, B) je řez v množině racionálních čísel.

Ukažme sporem, že (A, B) je reálné číslo, tj. že B nemá nejmenší prvek. Nechť b je nejmenší prvek množiny B. Pak $b^n > \alpha$ a podle 7.12 (b) existuje $c \in \mathbb{Q}$ takové, že $\alpha < c < b^n$. Protože množina racionálních čísel je hustě uspořádaná, existuje racionální číslo $f > 0$ splňující následující dvě podmínky:

$$f < \frac{b^n - c}{nb^{n-1}}, \quad f < \frac{\binom{n}{2i}}{\binom{n}{2i+1}} \cdot b \quad \text{pro libovolné } i \in \{1, \dots, m\},$$

kde

$$m = \begin{cases} \frac{n-2}{2} & \text{pro sudé } n, \\ \frac{n-1}{2} & \text{pro liché } n. \end{cases}$$

To znamená, že platí následující nerovnosti:

$$b^n - c - nfb^{n-1} > 0 \quad \text{a} \quad \tbinom{n}{2i} f^{2i} b^{n-2i} - \tbinom{n}{2i+1} f^{2i+1} b^{n-2i-1} > 0.$$

Položme $d = b - f$. Pak $d \in \mathbb{Q}$ a jelikož $b^n - c < b^n \leq nb^n$, je $\frac{b^n - c}{nb^{n-1}} < b$. Tedy $0 < d < b$.

Platí, že

$$\begin{aligned} d^n - c &= \sum_{i=0}^{n} \tbinom{n}{i} (-1)^i f^i b^{n-i} - c = \\ &= [(b^n - c) - nfb^{n-1}] + \sum_{i=1}^{m} \Big[\tbinom{n}{2i} f^{2i} b^{n-2i} - \tbinom{n}{2i+1} f^{2i+1} b^{n-2i-1} \Big] + F, \end{aligned}$$

kde

$$F = \begin{cases} f^n & \text{pro sudé } n, \\ 0 & \text{pro liché } n. \end{cases}$$

Jelikož výrazy v hranatých závorkách jsou z definice čísla f kladná racionální čísla, platí, že $d^n - c > 0$. Tudíž $\alpha < c < d^n$, odkud plyne $d \in B$. Ale $d < b$, což je spor. Množina B tedy nemá nejmenší prvek. Řez $\xi = (A, B)$ je proto nezáporným reálným číslem.

V následujícím ukážeme, že $\xi^n = \alpha$. Podle definice je $\xi^n = (\mathbb{Q} - C, C)$, kde $C = \{a_1 \cdot \ldots \cdot a_n \mid a_1, \dots, a_n \in B\}$. Zvolme $a_1, \dots, a_n \in B$ libovolně a označme a to nejmenší z nich. Pak $a_1 \ldots a_n \geq a^n$, přičemž z $a \in B$ plyne $a^n > \alpha$. Ukázali jsme, že $C \subseteq D$, kde $D = \{d \in \mathbb{Q} \mid d > \alpha\}$. Protože $\alpha = (\mathbb{Q} - D, D)$, tato inkluze znamená, že $\alpha \leq \xi^n$. Jestliže $\alpha < \xi^n$, existuje podle 7.12 (b) racionální číslo a takové, že $\alpha < a < \xi^n$. Podle lemmatu 8.1 existují racionální čísla $a_1, \dots, a_n$ taková, že $0 < a_i < \xi$ pro každé $i \in \{1, \dots, n\}$ a $a = a_1 \cdot \ldots \cdot a_n$.

Nechť $1 \leq h \leq n$ takové, že pro každé $i \in \{1, \dots, n\}$ máme $a_h \geq a_i$. Pak $\alpha < a \leq a_h^n < \xi^n$, z čehož plyne, že $a_h \in B$, odkud $a_h > \xi$, což je spor. Tudíž $\alpha = \xi^n$.

Případ $\alpha = 0$ plyne z tvrzení 6.18, případ $\alpha < 0$ se dokáže analogicky jako tvrzení 6.19.

8.3. Definice. Pro nezáporné $\alpha \in \mathbb{R}$ a přirozené n existuje podle věty 8.2 jediné řešení $\xi \geq 0$ binomické rovnice $x^n = \alpha$ v $\mathbb{R}$. Reálné číslo ξ se pak značí symbolem $\sqrt[n]{\alpha}$.

Je-li $\alpha \in \mathbb{R}, \alpha < 0$ a n přirozené liché číslo, pak binomická rovnice $x^n = \alpha$ má podle věty 8.2 právě jedno řešení ξ v $\mathbb{R}$. Pak klademe $\xi = \sqrt[n]{\alpha}$. V obou případech číslo $\sqrt[n]{\alpha}$ nazýváme *n-tá odmocnina z α*.

Zřejmě platí následující tvrzení.

8.4. Tvrzení. *Nechť $\alpha \in \mathbb{R}, \alpha \geq 0$, n liché přirozené číslo. Pak*

$$\sqrt[n]{-\alpha} = -\sqrt[n]{\alpha}.$$

Následující věta plyne přímo z věty 6.21 a udává nutnou a dostatečnou podmínku pro to, aby $\sqrt[n]{\alpha}$ byla racionálním číslem.

8.5. Věta. *Nechť je dáno reálné číslo α a přirozené číslo n. Nechť platí $\alpha > 0$ nebo platí, že $\alpha < 0$ a zároveň n liché. Pak reálné číslo $\sqrt[n]{\alpha}$ je racionálním číslem právě tehdy, když α je racionální číslo a $n \mid v_p(\alpha)$ pro každé prvočíslo p.*

V následující části si ukážeme, jak lze vyjádřit reálné číslo nekonečným tvarem složeným z „g-adických číslic". Budeme k tomu předpokládat jisté znalosti matematické analýzy, speciálně základní pojmy a tvrzení o nekonečných řadách.

Potřebujeme také zavést následující pojem.

8.6. Definice. Nechť α je reálné číslo. Podle věty 7.12 (b) a tvrzení 6.14 existují celá čísla a, b taková, že $a < \alpha < b$. Tudíž existuje největší celé číslo x takové, že $x \leq \alpha$. Číslo x se nazývá *celá část čísla* α a značíme jej $x = [\alpha]$. Číslo $\alpha - [\alpha]$ se označuje symbolem $\langle\alpha\rangle$ a nazývá se *necelá část čísla* α. Platí tedy

$$\alpha = [\alpha] + \langle\alpha\rangle, \quad [\alpha] \leq \alpha < [\alpha] + 1, \quad 0 \leq \langle\alpha\rangle < 1, \quad [\alpha] \in \mathbb{Z}.$$

V další části tohoto odstavce bude g značit přirozené číslo větší než 1.

8.7. Definice. Nechť pro celé nezáporné číslo n je $a_n \in \mathbb{Z}$ a pro $n \geq 1$ je $0 \leq a_n < g$. Nekonečná řada

$$\sum_{n=0}^{\infty} a_n g^{-n} = a_0 + \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots \qquad (*)$$

se nazývá *g-adický zlomek*, pro $n \geq 1$ se číslo a_n nazývá *g-adická číslice*. Místo zápisu $(*)$ se často používá zápis $a_0 + 0, a_1a_2a_3\ldots$ nebo $a_0, a_1a_2a_3\ldots$.

Z analýzy je známo, že řada $(*)$ konverguje a její součet α ($\alpha \in \mathbb{R}$) nazýváme *hodnota g-adického zlomku* $(*)$ a píšeme pak

$$\alpha = \sum_{n=0}^{\infty} \frac{a_n}{g^n}.$$

Říkáme též, že *g-adický zlomek* $(*)$ *je g-adickým rozvojem reálného čísla* α.

Jestliže existuje přirozené číslo N takové, že pro všechna $n > N$ je $a_n = 0$, pak se g-adický zlomek nazývá *konečný*, v opačném případě *nekonečný*.

Jestliže existuje celé nezáporné číslo N a přirozené číslo m tak, že pro libovolná celá čísla $l > N$, $k > N$, $l \equiv k (\mathrm{mod}\ m)$ platí $a_l = a_k$, nazývá se g-adický zlomek

$(*)$ *periodický*. Skupina g-adických číslic $a_{N+1}, a_{N+2}, \ldots, a_{N+m}$ se pak neustále opakuje a nazývá se *perioda*. Číslo m se nazývá *délka periody*. Píšeme pak

$$\alpha = a_0 + 0, a_1 \ldots a_N\overline{a_{N+1} \ldots a_{N+m}}.$$

8.8. Příklad. Provedeme-li zápis racionálního čísla $\alpha = \frac{113}{108}$ v desítkové soustavě ($g = 10$), dostaneme vyjádření $\alpha = 1,04629629629\cdots = 1,04\overline{629}$. Desetinný rozvoj je tedy nekonečný periodický s periodou délky 3.

Zapíšeme-li totéž číslo $\alpha = \frac{113}{108}$ jako g-adický zlomek pro $g = 6$, dostaneme $\alpha = 1 + \frac{0}{6} + \frac{1}{6^2} + \frac{4}{6^3} = 1,014$. Zlomek je v tomto případě konečný.

8.9. Věta. *Nechť α je libovolné reálné číslo. Pak α je hodnotou g-adického zlomku $\alpha = \sum_{n=0}^{\infty} a_n g^{-n}$, který není periodický s periodou $g-1$ délky 1. Toto vyjádření čísla α je jednoznačné.*

Důkaz. Pro libovolné reálné číslo α existuje posloupnost celých čísel $\{a_n\}_{n=0}^{\infty}$ a reálných čísel $\{\alpha_n\}_{n=0}^{\infty}$ taková, že platí: $a_0 = [\alpha]$, $\alpha_0 = \langle\alpha\rangle$, $a_n = [g\alpha_{n-1}]$, $\alpha_n = \langle g\alpha_{n-1}\rangle$ pro $n \geq 1$. Pak $\alpha = a_0 + \alpha_0$, $g\alpha_{n-1} = a_n + \alpha_n$, $0 \leq a_n < g$ pro $n \geq 1$, $0 \leq \alpha_n < 1$ pro $n \geq 0$. Tedy můžeme psát, že

$$\alpha = a_0 + \alpha_0 = a_0 + \frac{g\alpha_0}{g} = a_0 + \frac{[g\alpha_0]}{g} + \frac{\langle g\alpha_0\rangle}{g} = a_0 + \frac{a_1}{g} + \frac{\alpha_1}{g}.$$

Úplnou indukcí vzhledem k n se pak snadno ukáže, že pro každé celé číslo $n \geq 0$ platí:

$$\alpha = a_0 + \frac{a_1}{g} + \cdots + \frac{a_n}{g^n} + \frac{\alpha_n}{g^n},$$

odkud plyne $\alpha = \sum_{n=0}^{\infty} a_n g^{-n}$.

Ukažme nyní sporem, že uvažovaný g-adický zlomek není periodický s periodou $g-1$ délky 1. Předpokládejme, že existuje přirozené číslo N takové, že pro všechna celá čísla $n > N$ platí $a_n = g - 1$. Pak pro $n > N$ je $g\alpha_n = g - 1 + \alpha_{n+1}$, tudíž $1 - \alpha_n = \frac{1-\alpha_{n+1}}{g}$, odkud pro všechna $n > N$ a každé $k \in \mathbb{N}$ plyne indukcí vzhledem ke k, že

$$1 - \alpha_n = \frac{1 - \alpha_{n+k}}{g^k}.$$

Protože $\lim_{k\mapsto\infty} \frac{1-\alpha_{n+k}}{g^k} = 0$, je $1 - \alpha_n = 0$, což je spor, neboť $\alpha_n < 1$. Platí tedy, že g-adický zlomek $\sum_{n=0}^{\infty} a_n g^{-n}$ splňuje podmínky věty.

Na závěr dokažme sporem jednoznačnost takového vyjádření reálného čísla α. Nechť pro všechna celá čísla $n \geq 0$ jsou b_n celá čísla taková, že $0 \leq b_n < g$ pro $n \geq 1$, $\alpha = \sum_{n=0}^{\infty} b_n g^{-n}$ a neexistuje přirozené číslo N takové, že pro všechna $n > N$ je $b_n = g - 1$. Pro $n \geq 0$ položme

$$\beta_n = \sum_{k=1}^{\infty} \frac{b_{n+k}}{g^k}.$$

Jelikož existuje $k \geq 1$ takové, že $b_{n+k} \leq g-2$, je $0 \leq \beta_n < \sum_{k=1}^{\infty} \frac{g-1}{g^k} = 1$. Pro $n \geq 1$ platí $g\beta_{n-1} = \sum_{k=1}^{\infty} \frac{b_{n+k-1}}{g^{k-1}} = b_n + \beta_n$, z čehož vyplývá, že $b_n = [g\beta_{n-1}]$ a $\beta_n = \langle g\beta_{n-1}\rangle$. Jelikož máme $\beta_0 = \alpha - b_0$, je $b_0 = [\alpha]$, $\beta_0 = \langle\alpha\rangle$, odkud již vyplývá, že $a_n = b_n, \alpha_n = \beta_n$ pro libovolné $n \geq 0$. Tím je věta dokázána.

8.10. Příklad. Vezměme reálné číslo α, jehož g-adický rozvoj pro $g = 10$ vypadá následovně:

$$\alpha = 1 + \tfrac{2}{10} + \tfrac{9}{10^2} + \tfrac{9}{10^3} + \tfrac{9}{10^4} + \cdots = 1,2\overline{9}.$$

Tento g-adický zlomek je periodický s periodou $g-1 = 9$ délky 1. Podle předchozí věty však je číslo α hodnotou g-adického zlomku, který nemá tyto vlastnosti.

Skutečně, součet geometrické řady

$$\tfrac{9}{10^2} + \tfrac{9}{10^3} + \tfrac{9}{10^4} + \ldots$$

s kvocientem $q = \frac{1}{10}$ je roven $\frac{1}{10}$. Proto číslo α lze psát ve tvaru

$$\alpha = 1 + \tfrac{2}{10} + \tfrac{1}{10} = 1 + \tfrac{3}{10} = 1,3.$$

8.11. Věta. *Nechť α je reálné číslo. Následující výroky jsou ekvivalentní:*

(a) *α je racionální číslo,*

(b) *každý g-adický rozvoj reálného čísla α je periodický,*

(c) *existuje periodický g-adický rozvoj reálného čísla α.*

Důkaz. „(c) $\Longrightarrow$ (a)" Nechť existuje periodický g-adický rozvoj reálného čísla α. Pak $\alpha = b + c\sum_{n=1}^{\infty} \frac{1}{g^{mn}}$, kde b, c jsou racionální čísla a m délka periody nějakého periodického g-adického rozvoje α. Tudíž

$$\alpha = b + \frac{c}{g^m - 1},$$

což znamená, že α je racionální číslo.

„(a) $\Longrightarrow$ (b)" Nechť α je racionální číslo. Existuje posloupnost celých čísel $\{a_n\}_{n=0}^{\infty}$ a reálných čísel $\{\alpha_n\}_{n=0}^{\infty}$ tak, že platí: $a_0 = [\alpha]$, $\alpha_0 = \langle\alpha\rangle$, $a_n = [g\alpha_{n-1}]$, $\alpha_n = \langle g\alpha_{n-1}\rangle$ pro libovolné $n \geq 1$. Podle důkazu věty 8.9 je pak $\alpha = a_0 + \alpha_0$, $g\alpha_{n-1} = a_n + \alpha_n, 0 \leq a_n < g$ pro $n \geq 1$, $0 \leq \alpha_n < 1$ pro $n \geq 0$ a platí

$$\alpha = \sum_{n=0}^{\infty} \frac{a_n}{g^n}.$$

Pak α_n je racionální číslo pro libovolné $n \geq 0$. Položme $r_n = \alpha_n \cdot m$, kde $\alpha = \frac{r}{m}$, $r, m \in \mathbb{Z}$, $m > 0$. Odtud pro $n \geq 0$ dostáváme, že $0 \leq r_n < m$, $r = ma_0 + r_0$, $gr_{n-1} = a_n m + r_n$ pro $n \geq 1$. Z toho plyne, že pro $n \geq 0$ je r_n celé číslo a pro $n \geq 1$ je $a_n = [\frac{gr_{n-1}}{m}]$ a $a_0 = [\frac{r}{m}]$. Podle věty 4.18 existují různá přirozená čísla ν, μ taková, že $r_\nu = r_\mu$, odkud plyne, že g-adický zlomek $\sum_{n=0}^{\infty} a_n g^{-n}$ je periodický.

Tudíž výrok (a) implikuje, že g-adický rozvoj reálného čísla α s vlastnostmi z věty 8.9 je periodický. Odtud a z věty 8.9 plyne dokazované tvrzení.

„(b) $\Longrightarrow$ (c)" Platnost této implikace je zřejmá.

8.12. Poznámka. V praxi se používá nejčastěji $g = 10$, dostáváme pak tzv. *desetinný* neboli *dekadický rozvoj*. Ve výpočetní technice se často užívá $g = 2$.

8.13. Cvičení.

1) Napište následující g-adické zlomky v desítkové soustavě:

a) $0,1001101$ $(g = 2)$,

b) $0,102$ $(g = 3)$,

c) $0,73$ $(g = 9)$.

2) Napište číslo $0,4140625$ ve tvaru g-adického zlomku:

a) $g = 2$,

b) $g = 8$.

3) Převeďte následující čísla přímo z dvojkové do šestnáctkové soustavy, resp. naopak (přímo znamená bez toho, abyste je zapisovali v desítkové soustavě):

a) $0,0110100001$ $(g = 2)$,

b) $10001,10011110101$ $(g = 2)$,

c) $C3,4E$ $(g = 16)$.

Při zápisu čísel v šestnáctkové soustavě používáme místo číslic $10 - 15$ velkých písmen $A - F$.

4) Dokažte, že číslo

$$0,123456789101112131415\ldots$$

není racionální.

5) Rozhodněte, zda existuje necelé reálné číslo takové, že v desítkové i trojkové soustavě je jeho g-adický rozvoj konečný.