4.3. **Podílová tělesa.**

Tak jako lze obor celých čísel rozšířit do tělesa racionálních čísel, každý obor integrity $\mathbf{R}$ lze rozšířit na tzv. *podílové těleso*, které lze zkonstruovat jako „těleso zlomků", jejichž čitatel i jmenovatel jsou prvky daného oboru. Podílová tělesa hrají v komutativní algebře důležitou roli, jak uvidíme například v Sekci 9, kde nám budou nástrojem k důkazu Gaussovy věty.

Konstrukce probíhá následujícím způsobem. Definujeme relaci $\sim$ na množině $R \times (R \setminus \{0\})$ předpisem

$$(a,b) \sim (c,d) \iff ad = bc.$$

Není těžké nahlédnout, že jde o ekvivalenci: reflexivita je zřejmá, symetrie plyne z komutativity násobení a tranzitivitu získáme následujícím výpočtem: je-li $(a,b) \sim \sim (c,d) \sim (e,f)$, tedy $ad = bc$ a $cf = de$. Pak ale $adf = bcf = bde$, a tedy $af = be$, protože $d \neq 0$ (ke krácení potřebujeme předpoklad, že $\mathbf{R}$ je obor integrity!).

Pro jednoduchost vyjadřování budeme značit blok $[(a,b)]_\sim$ této ekvivalence jako zlomek $\frac{a}{b}$. Uvažujme množinu Q všech bloků této ekvivalence (tj. všech zlomků) a definujme na ní operace

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad -\frac{a}{b} = \frac{-a}{b}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad 0 = \frac{0}{1}, \qquad 1 = \frac{1}{1}.$$

(Aby jmenovatel zůstal nenulový, potřebujeme předpoklad, že $\mathbf{R}$ je obor integrity!)

Tvrzení 4.4. *Množina Q s právě definovanými operacemi tvoří těleso, tzv.* podílové těleso *oboru* $\mathbf{R}$.

Důkaz. Ověříme postupně všechny axiomy:

- Asociativita sčítání: $\frac{a}{b}+(\frac{c}{d}+\frac{e}{f}) = \frac{a}{b}+\frac{cf+de}{df} = \frac{adf+b(cf+de)}{bdf} = \frac{adf+bcf+bde}{bdf} = = \frac{ad+bc}{bd} + \frac{e}{f} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$.
- Komutativita sčítání: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$.
- Nula: $\frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1+b\cdot 0}{b\cdot 1} = \frac{a}{b}$.
- Odčítání: $\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-ab)}{b^2} = \frac{0}{b^2} = 0$.
- Asociativita a komutativita násobení plyne okamžitě z týchž vlastností oboru $\mathbf{R}$.
- Jednotka: $\frac{a}{a} \cdot \frac{1}{1} = \frac{a\cdot 1}{a\cdot 1} = \frac{a}{a}$.
- Distributivita: $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{acf+ade}{bdf} = \frac{abcf+abde}{b^2df} = \frac{ac}{bd} + \frac{ae}{bf}$.

Navíc $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$ pro každé $\frac{a}{b} \neq 0$, čili $\mathbf{Q}$ je těleso. □

Příklady.

- Podílové těleso oboru $\mathbb{Z}$ je těleso $\mathbb{Q}$.
- Podílové těleso oboru $\mathbb{Z}[i]$ je těleso $\mathbb{Q}(i)$, sestávající ze všech čísel $a + bi$, $a, b \in \mathbb{Q}$.
- Podílové těleso oboru $\mathbf{R}[x]$ je těleso racionálních funkcí nad $\mathbf{R}$.

5. Základní pojmy teorie dělitelnosti

Cíl. *Ujasníme si, které prvky jsou z hlediska dělitelnosti nerozlišitelné (relace asociovanosti, souvislost s invertibilními prvky), což nám umožní na relaci dělitelnosti pohlížet jako na uspořádání. Zavedeme největší společný dělitel a definujeme analogii k pojmu prvočísla, tzv. ireducibilní prvky.*

V celé sekci budeme uvažovat nějaký pevně daný obor integrity $\mathbf{R}$.

5.1. Invertibilní prvky.

Definice. Řekneme, že a *dělí* b v oboru $\mathbf{R}$ (píšeme $a \mid b$), pokud existuje $c \in R$ takové, že $b = ac$. Řekneme, že prvky a a b jsou *asociované* (píšeme $a \parallel b$), pokud $a \mid b$ a $b \mid a$. Prvek a se nazývá *invertibilní*, pokud $a \parallel 1$, tj. existuje b takové, že $ab = 1$; toto b obvykle značíme a^{-1}. Dělitel prvku a se nazývá *vlastní*, jestliže není asociovaný ani s 1, ani s a.

Tvrzení 5.1. *Dva prvky a, b jsou asociované právě tehdy, když existuje invertibilní prvek q takový, že $a = bq$.*

Důkaz. ($\Leftarrow$) Protože $a = bq$, platí $b \mid a$. Protože taky $b = aq^{-1}$, platí $a \mid b$.

($\Rightarrow$) Protože $b \mid a$, můžeme psát $a = bu$, a protože $a \mid b$, můžeme psát $b = av$, pro nějaká u, v. Tedy $a = bu = avu$ a krácením dostáváme $uv = 1$, čili $u, v \parallel 1$. □

Příklady.

- V tělese je každý nenulový prvek invertibilní. Tedy $a \parallel b$ pro každé $a, b \neq 0$.
- V oboru $\mathbb{Z}$ jsou invertibilní pouze prvky ± 1. Tedy $a \parallel b$ právě tehdy, když $a = \pm b$.
- V oboru $\mathbb{Z}[i]$ jsou invertibilní pouze prvky $\pm 1, \pm i$. Tedy $a \parallel b$ právě tehdy, když $a = \pm b$ nebo $a = \pm ib$.
- V oboru $\mathbb{Z}[i\sqrt{2}]$ jsou invertibilní pouze prvky ± 1. Tedy $a \parallel b$ právě tehdy, když $a = \pm b$.
- V oboru $\mathbf{R}[x]$ jsou invertibilní právě polynomy stupně 0, jejichž člen je invertibilní v oboru $\mathbf{R}$.

Příklad. Pozor na následující záludnost!

- $3x+6 \parallel x+2$ v oboru $\mathbb{Q}[x]$, protože $3x+6 = 3 \cdot (x+2)$ a $x+2 = \frac{1}{3} \cdot (3x+6)$;
- $3x + 6 \nparallel x + 2$ v oboru $\mathbb{Z}[x]$, protože $\frac{1}{3} \notin \mathbb{Z}[x]$.