5. cvičení

Ve škole:

1. Nechť p a q jsou dva nenulové polynomy nad tělesem T. Dokažte tvrzení:

(a) Jestliže p dělí q a zároveň q dělí p, pak existuje nenulový prvek v tělesa T, pro který $p = vq$.

(b) Největší společný dělitel p a q je určen jednoznačně až na násobek nenulovým prvkem tělesa.

2. Uvažujme obor integrity $(R, +, \cdot, -, 0, 1)$ a označme $(Q, +, \cdot, -, \frac{0}{1}, \frac{1}{1})$ jeho podílové těleso. Ověřte, že

(a) $\frac{a \cdot x}{b \cdot x} = \frac{a \cdot y}{b \cdot y}$ pro každé $\frac{a}{b} \in Q$ a $x, y \in R \setminus \{0\}$,

(b) jsou operace na podílovém tělese dobře definované.

3. Dokažte, že podílové těleso oboru $\mathbb{Z}[i]$ lze ztotožnit s tělesem $\mathbb{Q}[i]$ (nejprve tvrzení přesně zformulujte!).

Úlohy pro samostatné počítání:

4. Dokažte, že je podílové těleso $(Q, +, \cdot, -, \frac{0}{1}, \frac{1}{1})$ opravdu těleso.

5. Kdybychom symbolem $\frac{a}{b}$ označili nikoli třídu ekvivalence, nýbrž dvojici $(a, b) \in R \times (R \setminus \{0\})$ a kdybychom operace $+, -, \cdot$ zavedli stejně jako u podílových těles, které axiomy oboru integrity by pro $R \times (R \setminus \{0\})$ neplatily?

Řešení:

1. (a) Protože p dělí q existuje polynom u, pro který $q = up$, a podobně protože q dělí p existuje polynom v, pro který $p = vq$. Dosadíme-li do druhého vztahu za q dostáváme $p = vup$, proto $p(1 - vu) = 0$ a tudíž $1 - vu = 0$, neboť $T[x]$ je obor. Protože $1 = vu$, musí být u i v nutně polynomy stupně nula, tedy $u, v \in T^*$.

   (b) Nechť a je nějaký největší společný dělitel p a q a b je největší společný dělitel p a q získaný Eukleidovým algoritmem. Protože $b = up + vq$, kde u a v jsou Bézoutovy koeficienty, musí a dělit b, tedy $b = ua$ pro vhodný polynom u. Protože z definice jsou polynomy a a b z definice stejného stupně, musí být u nutně stupně nula, tedy $u \in T \setminus \{0\}$.

2. (a) $\frac{a \cdot x}{b \cdot x} = \frac{a \cdot y}{b \cdot y} \Leftrightarrow (a \cdot x, b \cdot x) \sim (a \cdot y, b \cdot y) \Leftrightarrow axby = bxay$, což plyne z komutativity násobení.

   (b) nechť $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ a $\frac{c_1}{d_1} = \frac{c_2}{d_2}$, pak $\frac{a_1}{b_1} \cdot \frac{c_1}{d_1} = \frac{a_1 c_1}{b_1 d_1} = \frac{a_1 c_1 b_2 d_2}{b_1 d_1 b_2 d_2} = \frac{a_2}{b_2} \cdot \frac{c_2}{d_2}$ a $\frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_1 d_1 + b_1 c_1}{b_1 d_1} = = \frac{a_1 b_2 d_1 d_2 + b_1 b_2 d_2 c_1}{b_1 d_1 b_2 d_2} = \frac{a_2 b_1 d_1 d_2 + b_1 b_2 d_1 c_2}{b_1 d_1 b_2 d_2} = \frac{a_2}{b_2} + \frac{c_2}{d_2}$.

3. Zobrazení, které formálnímu zlomku $\frac{a+bi}{c+di}$, kde $a, b, c, d \in \mathbb{Z}$, $b \neq 0 \neq d$, přiřadí jeho komplexní vyhodnocení

   $$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i \in \mathbb{Q}[i] \subseteq \mathbb{C}$$

   je izomorfismus podílového tělesa oboru $\mathbb{Z}[i]$ a tělesa $\mathbb{Q}[i]$.

4. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$,

   $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{adf+b(cf+de)}{bdf} = \frac{(ad+bc)f+bde}{bdf} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$,

   $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{a(ce)}{bdf} = \frac{(ac)e}{bdf} = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$,

   $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b} = \frac{a}{b}$, $\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b} = \frac{a}{b}$, $\frac{a}{b} + \frac{-a}{b} = \frac{a+(-a)}{bb} = \frac{0}{bb} = \frac{0}{1}$,

   $\frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{acbf+bdae}{bdbf} = \frac{acf+ade}{bdf} = \frac{a}{b} \cdot \frac{cf+de}{df} = \frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f})$.

5. Platily by všechny axiomy kromě axiomu opačného prvku a axiomu distributivity.