LAG1, ZS 2018/19

T. Macko, M. Sleziak

Prednáškové úlohy 6

06.11.2018

Úloha 6 pokračuje na druhej strane.

1. V okruhu $(\mathbb{Z}[t], +, \cdot)$ ako na prednáške spočítajte
$$(1+3t^2+2t^3)+(2+4t-t^2+2t^3),\ (1+3t^2+2t^3)\cdot(2+4t-t^2+2t^3),$$
$$(1-t)\cdot(1+t+t^2+t^3+t^4),\ (1-t)\cdot(1+2t+3t^2+4t^3+5t^4)$$

2. 1.7.8 (4) Prečo okruh polynómov $\mathbb{R}[t]$ nie je poľom?

3. V okruhu $(\mathbb{Z}_5, +, \cdot)$ vypočítajte
$$2\cdot 3^{-1},\ 3\cdot 2^{-1},\ 1+4\cdot 3,\ 4\cdot 4^{-1},\ 4\cdot 3^{-1},\ 3+2\cdot 4^{-1}.$$

4. Napíšte tabuľku multiplikatívnych grúp
$$((\mathbb{Z}_2)^*, \cdot),\ ((\mathbb{Z}_3)^*, \cdot),\ ((\mathbb{Z}_7)^*, \cdot).$$
Ak $m = 2, 3, 7$ aký je vzťah medzi $((\mathbb{Z}_m)^*, \cdot)$ a $(\mathbb{Z}_{m-1}, +)$. Odôvodnite.

5. Ukážte, že množina $\mathbb{Q}(\sqrt{2}) = \{x + y\cdot\sqrt{2} \mid x, y \in \mathbb{Q}\} \subset \mathbb{R}$ s operáciami $+$ a $\cdot$ zdedenými z $\mathbb{R}$ je okruh s 1. Je $\mathbb{Q}(\sqrt{2})$ pole?

6. Nech $m \geq 2$. Uvažujme množinu $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, s operáciami:
$$\begin{aligned} +_m\colon \mathbb{Z}_m\times\mathbb{Z}_m \to \mathbb{Z}_m &\quad x +_m y = r\ x+y = k\cdot m + r,\ 0\le r\le m-1\\ \cdot_m\colon \mathbb{Z}_m\times\mathbb{Z}_m \to \mathbb{Z}_m &\quad x \cdot_m y = s\ x\cdot y = l\cdot m + s,\ 0\le s\le m-1. \end{aligned}$$
Ukážte, že $(\mathbb{Z}_m, +_m, \cdot_m, 1)$ je komutatívny okruh s jednotkou.

Uvažujme ďalej množinu $\mathbb{Z}/m\mathbb{Z} = \{[x] \mid x \in \mathbb{Z}\}$, kde príslušná relácia ekvivalencie je daná predpisom $x \sim y \ \Leftrightarrow x - y = m\cdot k$ pre nejaké $k \in \mathbb{Z}$, takže máme $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$ s operáciami:
$$\begin{aligned} +\colon \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} &\quad [x]+[y] = [x+y]\\ \cdot\colon \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} &\quad [x]\cdot[y] = [x\cdot y]. \end{aligned}$$
Ukážte, že tieto operácie su dobre definované a že $(\mathbb{Z}/m\mathbb{Z}, +, \cdot, [1])$ je komutatívny okruh s jednotkou.

Ukážte, že pre funkciu
$$\overline{q}_m\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_m \quad x \mapsto r, \quad \text{kde } x = k\cdot m + r,\ 0\le r\le m-1,$$

o ktorej už vieme, že je izomorfizmom abelovských grúp $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_m$ platí

$$\overline{q}_m([x] \cdot [y]) = \overline{q}_m([x]) \cdot_m \overline{q}_m([y]).$$

(Teda $\overline{q}_m$ je funkcia zo $\mathbb{Z}/m\mathbb{Z}$ do $m\mathbb{Z}$, ktorá rešpektuje sčítanie a násobenie a je bijektívna. Takáto funkcia sa nazýva *izomorfizmus okruhov*. Z jej existencie vyplýva, že okruhy $(\mathbb{Z}_m, +_m, \cdot_m, 1)$ a $(\mathbb{Z}/m\mathbb{Z}, +, \cdot, [1])$ majú zhodné okruhovo teoretické vlastnosti, hovoríme, že sú izomorfné ako okruhy. Špeciálne, jeden z nich je pole práve vtedy keď druhý z nich je pole.)