1. cvičení

1. Rozhodněte, zda je

(a) množina $\mathbb{Z} \times \mathbb{Z}$ se standardními operacemi $+, -, \cdot$ po složkách,

(b) množina $\mathbb{Z}$ se standardními operacemi $+, -$ a s operací $x \cdot y = 0$,

(c) množina $P(X) = (\{Y : Y \subseteq X\}, \triangle, -, \cap, \emptyset)$ s operacemi symetrické diference $\triangle$, průniku $\cap$ a s odčítáním $-Y = Y$,

(d) $(\mathbb{Q}^+, \cdot, ^{-1}, +, 1)$, kde $\mathbb{Q}^+ = \{a \in \mathbb{Q} : a > 0\}$,

komutativním okruhem s jednotkou, oborem integrity nebo tělesem.

2. Rozhodněte, zda následující podmnožiny tvoří podokruh tělesa $\mathbb{C}$:

$$\{a + b\sqrt{2} :\ a, b \in \mathbb{Z}\}, \quad \{a + b\sqrt[3]{2} :\ a, b \in \mathbb{Z}\}, \quad \{a + b\zeta :\ a, b \in \mathbb{Z}\},$$

$$\{a + b\omega :\ a, b \in \mathbb{Z}\}, \quad \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} :\ a, b, c, d \in \mathbb{Z}\},$$

kde $\zeta = e^{\pi i/4}$ a $\omega = e^{2\pi i/3}$.

Návod: Všimněte si, že $\omega^2 = -1 - \omega$.

3. Rozhodněte, zda následující podmnožiny tvoří podtěleso tělesa $\mathbb{C}$:

$$\{a + b\sqrt{2} :\ a, b \in \mathbb{Q}\}, \quad \{a + b\sqrt[3]{2} + c\sqrt[3]{4} :\ a, b \in \mathbb{Q}\}, \quad \{a + b\omega :\ a, b \in \mathbb{Q}\},$$

kde $\omega = e^{2\pi i/3}$.

4. Dokažte, že komutativita sčítání plyne z ostatních axiomů komutativních okruhů s jednotkou.

5. Dokažte pro libovolnou asociativní operaci $*$ na množině A, že hodnota výrazu $a_1 * a_2 * \cdots * a_n$ pro $a_1, \ldots, a_n \in A$ nezáleží na uzávorkování.

Řešení:

1. (a), (c) jsou okruhy, nikoli obory ani tělesa (s výjimkou $|X| = 1$ v (c)), (b),(d) nejsou ani okruhy (neexistuje jednotka).

2. $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$ ani $\{a + b\zeta : \ a, b \in \mathbb{Z}\}$ nejsou podokruhy, ostatní množiny jsou.

3. všechny tři množiny jsou podtělesa tělesa $\mathbb{C}$.

4. Využijeme-li distributivity dostaneme:

$$(1 + a)(1 + b) = (1 + a)1 + (1 + a)b = 1 + a + b + ab,$$

$$(1 + b)(1 + a) = (1 + b)1 + (1 + b)a = 1 + b + a + ba,$$

   Díky komutativitě násobení platí, že

$$1 + a + b + ab = 1 + b + a + ab$$

   a zbývá odečíst prvek 1 zleva a prvek ab zprava.

5. Indukcí podle n dokážeme, že každý výraz s hodnotami $a_1, \dots, a_n \in A$ je roven výrazu $a_1 * (a_2 * (a_3 * (\cdots * a_n) \dots))$. Pro $n \leq 3$ to zřejmě platí. Nechť $n > 3$. Máme-li výraz tvaru $a_1 * u$, kde u je výraz délky $n - 1$, pak u je roven požadovanému tvaru podle indukčního předpokladu, a tudíž tvrzení platí. V opačném případě lze výraz napsat ve tvaru $(u * v) * w$, kde u jsou výrazy kratší než n, tedy $u = a_1 * z$ pro vhodný výraz z podle indukčního předpokladu, proto z asociativity plyne

$$(u * v) * w = u * (v * w) = (a_1 * z) * (v * w) = a_1 * (z * (v * w)).$$

   Závěr nyní dostaneme úvahou z první části důkazu.