2. cvičení

Ve škole:

1. Popište všechny invertibilní prvky okruhu $\mathbb{Z}_n$ s operacemi modulo n a rozhodněte, pro která n je $\mathbb{Z}_n$ obor integrity a pro která je těleso. Najděte v $\mathbb{Z}_{100}$ inverz k prvku 77.

2. Dokažte, že je konečný obor nutně těleso.

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

$\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}, \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}, \{a+b\sqrt[3]{2} \mid a,b \in \mathbb{Z}\}, \{a+b\omega \mid a,b \in \mathbb{Z}\},$

$$\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q}\}, \quad \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Z}\},$$

kde $\omega = e^{2\pi i/3}$. Které z podokruhů tvoří tělesa? (Všimněte si, že $\omega^2 = -1-\omega$.)

4. Popište nejmenší podokruh s jednotkou maticového okruhu $M_2(\mathbb{Z})$, který obsahuje prvek $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Tvoří tento podokruh komutativní okruh?

Úloha pro samostatné počítání:

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

Řešení:

1. Invertibilní jsou právě prvky nesoudělné s n. $77^{-1} = 13$.

   $\mathbb{Z}_n$ je obor integrity $\Leftrightarrow$ je těleso $\Leftrightarrow$ je n prvočíslo.

2. Nechť R je konečný obor. Uvážíme pro každý nenulový prvek $a \in R$ zobrazení $\tau_a : R \to R$ dan0 vyta $\tau(r) = a \cdot r$. Jestliže $\tau(r) = \tau(s)$, pak $a \cdot (r - s) = 0$, a proto $r = s$. Tedy τ_a je prosté zobrazení konečné množiny do sebe, a tudíž i zobrazení na. Tudíž $a^{-1} = \tau_a^{-1}(1)$.

3. $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$ není podokruh, ostatní množiny jsou, z toho $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b \in \mathbb{Q}\}$ a $\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ tvoří tělesa

4. $\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid | \ a, b \in \mathbb{Z}\}$, tento podokruh tvoří komutativní okruh.

5. $\{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Z}\}$ není podokruh, ostatní množiny jsou, z toho $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : \ a, b \in \mathbb{Q}\}$ a $\{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ tvoří tělesa

6. $\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid | \ a, b \in \mathbb{Z}\}$, tento podokruh tvoří komutativní okruh.

7. 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.