7. Abelovy grupy, okruhy a tělesa

1. Maticí řádu n rozumíme čtvercovou matici $n \times n$. Trojúhelníkovou maticí řádu n rozumíme matici (a_{ij}) řádu n, ve které $a_{ij} = \mathbf{0}$ pro $i > j$. Ukažte, že množina $R_{(n)}$ matic řádu n, kde prvky matic jsou z okruhu R, tvoří okruh. Ověřte, že množina trojúhelníkových matic řádu n je podokruh $R_{(n)}$.

2. Buď $n \geq 1$. Nalezněte alespoň jeden injektivní homomorfismus z $R_{(n)}(+, \mathbf{0})$ do $R_{(2n)}(\cdot, \mathbf{1})$.

3. Dokažte, že $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ a $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ generují okruh $\mathbf{Z}_{(2)}$.

4. Buď B podmnožina Abelovy grupy $A(+, -, \mathbf{0})$. Dokažte, že podgrupa grupy A generovaná B je rovna $\{\sum_{1 \leq i \leq n} k_i b_i;\ b_i \in B,\ k_i \in \mathbb{Z},\ n \in \mathbf{N}_0\}$.

5. Buď $(M, \leq)$ lineárně uspořádaná množina a ať pro všechna $m \in M$ je $A_m = A_m(\omega_1, \dots, \omega_n)$ algebra. Jestliže A_m je podalgebra $A_{m'}$ pro všechna $m, m' \in M$ taková, že $m \leq m'$, ukažte, že na $A = \cup(A_m;\ m \in M)$ lze definovat operace $\omega_1, \dots, \omega_n$ tak, že A_m je podalgebra A pro každé $a \in A$.

6. Zjistěte, které z následujících množin jsou podokruhy $\mathbb{R}$:

(i) $\{m + n\sqrt{5};\ m, n \in \mathbb{Z}\}$,
(ii) $\{m + n\sqrt[3]{5};\ m, n \in \mathbb{Z}\}$,
(iii) $\{k + m\sqrt[3]{2} + n\sqrt[3]{4};\ k, m, n \in \mathbb{Z}\}$.

7. Ověřte, že je-li A Abelova grupa a $f, g \in \mathrm{End}(A)$, tak $f + g \in \mathrm{End}(A)$ a $-f \in \mathrm{End}(A)$. (Je $(f+g)(x) = f(x) + g(x)$ a $(-f)(x) = -(f(x))$ pro všechna $x \in A$.) Ukažte, že $\mathrm{End}(A)$ lze považovat za okruh. Co je $\mathbf{0}_{\mathrm{End}(A)}$ a co je $\mathbf{1}_{\mathrm{End}(A)}$?

8. Ukažte, že definujeme-li na $D = \{0, 1\}$ binární operace $+$ a $\cdot$ tak, že $0 + 0 = 1 + 1 = 0 \cdot 1 = 1 \cdot 0 = 0 \cdot 0 = 0$ a $1 + 0 = 0 + 1 = 1 \cdot 1 = 1$, a unární operaci $-$ tak, že $-0 = 0$ a $-1 = 1$, tak $D(+, \cdot, -, 0, 1)$ je těleso. Uvědomte si, že zobrazení $0 \to \mathrm{F}$, $1 \to \mathrm{T}$ indukuje na $\mathit{Bool} = \{\mathrm{T}, \mathrm{F}\}$ také strukturu tělesa. Jaká je 'logická' interpretace operací $\cdot$, $+$ a $-$?

9. Ukažte, že každou Abelovu grupu A, ve které pro všechna $a \in A$ platí $a + a = 0$, lze považovat za vektorový prostor nad tělesem D z předchozího cvičení. Co jsou pak endomorfismy Abelovy grupy A ve vztahu k tomuto vektorovému prostoru?

10. Buď A Abelova grupa izomorfní Kleinově grupě. Určete řád $\mathrm{End}(A)$.

11. Buď $f : R \to S$ homomorfismus okruhů. Ukažte, že $f(n \cdot a) = n \cdot f(a)$ pro každé $n \in \mathbb{Z}$.

12. Pro $d \in \mathbb{Q}$ označme $\mathbb{Q}(\sqrt{d})$ množinu $\{a + b\sqrt{d};\ a, b \in \mathbb{Q}\}$. Ukažte, že $Q(\sqrt{d})$ je podtěleso $\mathbb{R}$.

13. Ukažte, že tělesa $\mathbb{Q}(\sqrt{7})$ a $\mathbb{Q}(\sqrt{11})$ nejsou izomorfní.

14. Ukažte, že pravé ideály okruhu R tvoří uzávěrový systém.

15. Ukažte, že netriviální okruh R je těleso právě když nemá žádný vlastní levý ideál ani žádný vlastní pravý ideál.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Řešení

1. Ověření axiomů okruhu se pro matice nad (obecným) okruhem R provede stejně jako pro matice nad číselnými tělesy (kde jde o běžně známé identity).

Ať $C = AB$, kde $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$, takže $c_{ij} = \sum_k a_{ik}b_{kj}$. Je-li $i > j$, je $k > j$ nebo $i > k$, takže součin trojúhelníkových matic je opět trojúhelníková matice. Trojúhelníkové matice tedy tvoří podmnožinu, která je uzavřena na násobení, sčítání a opačné matice, a obsahuje nulovou i jednotkovou matici. Proto jde o podokruh $R_{(n)}$.

2. Ať $E \in R_{(n)}$ je jednotková matice. Hledané zobrazení je například
$A \to \begin{pmatrix} E & A \\ 0 & E \end{pmatrix}$.

3. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$,
$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$,
$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$,
$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$,
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + c \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + d \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

4. Uvedenou množinu označme U a ať V značí podgrupu grupy A generovanou množinou B. Součtem nulové délky se (podle běžné konvence) dostane nulový prvek, takže je $\mathbf{0} \in U$. Jistě je $U \subseteq V$, takže stačí ukázat, že U je podgrupa A. Jsou-li $u, v \in U$, tak existuje konečná podmnožina $B' \subseteq B$ taková, že $u = \sum u_b b$ a $v = \sum v_b b$, kde b probíhá B' a u_b, v_b jsou celá čísla. Přitom $u + v = \sum (u_b + v_b) b$ i $-u = \sum (-u_b) b$ leží v U, takže U je uzavřeno na všechny tři operace.

5. Ať $\omega = \omega_j$, $1 \le j \le n$, je operace četnosti k. Chceme-li definovat $\omega(a_1, \dots, a_k)$ na A tak, aby každé A_m, $m \in M$, bylo uzavřené na ω, stačí uvážit, že pro libovolná $a_1, \dots, a_k$ existuje $m \in M$ takové, že platí $\{a_1, \dots, a_k\} \subseteq A_m$, takže musí být $\omega_A(a_1, \dots, a_k) = \omega_{A_m}(a_1, \dots, a_k)$. Tato definice je korektní, neboť pro $\{a_1, \dots, a_k\} \subseteq A'_m$ je $m \le m'$ nebo $m' \le m$, takže platí $A_m \subseteq A_{m'}$ nebo $A_{m'} \subseteq A_m$, a proto je $\omega_{A_m}(a_1, \dots, a_k) = \omega_{A_{m'}}(a_1, \dots, a_k)$.

6. (i) ano, (ii) ne, (iii) ano.

7. $\mathbf{0}_{\mathrm{End}(A)}$ je zobrazení $a \to \mathbf{0}_A$ a $\mathbf{1}_{\mathrm{End}(A)}$ je zobrazení $a \to a$, pro všechna $a \in A$.

8. $+$ odpovídá logickému XOR, $\cdot$ odpovídá logickému AND a $-$ odpovídá negaci.

9. Jsou to lineární zobrazení.

10. Protože endomorfismy jsou lineární zobrazení (viz cvičení 9), je jich tolik, kolik je matic nad D řádu 2. A těch je 16.

13. Využijte toho, že rovnice $x^2 = 7$ má řešení v $\mathbb{Q}(\sqrt{7})$, ale ne v $\mathbb{Q}(\sqrt{11})$.