ALG2 – 5. cvičení

1. Dokažte, že množina všech čtvercových matic typu n×n nad **Z** tvoří okruh vzhledem k maticovému sčítání a násobení.

Řešení:

Pozn. Ověřujeme vždy podmínky pro jednotlivé třídy matic, např. matic o velikosti 2×2, o velikosti 3×3, atd. Víme totiž, že nemůžeme čtvercové matice o různé velikosti sčítat ani násobit mezi sebou!

$(M_n, +, \cdot)$

Ověřujeme následující podmínky:

- $(M_n, +)$ musí být **abelovská grupa** (uzavřenost vůči operaci +, jednotkový prvek, inverzní prvky, komutativita, asociativita).
- $(M_n, \cdot)$ musí být **pologrupa** (uzavřenost vůči operaci, asociativita).
- musí platit **distributivní zákony**.

$(M_n, +)$

- je zjevně uzavřená vůči + (sčítáním dvou matic získáme vždy matici o stejném rozměru)
- jednotkovým prvkem je nulová matice o rozměru n×n
- asociativní je díky asociativitě sčítání celých čísel
- inverzní prvky existují (pro $x \in \mathbf{Z}$ je inverzním prvkem -x)
- komutativita vyplývá z komutativity sčítání celých čísel

⇨ abelovská grupa

$(M_n, \cdot)$

- je uzavřená vůči operaci ·, jelikož násobením dvou čtvercových matic vždy získáme čtvercovou matici o stejném rozměru
- je asociativní – snadno lze ověřit vynásobením nějakých obecných čtvercových matic A, B, C, viz podrobnější důkaz níže:

Column J of (AB)C is equal to AB times column J of C. This is equal to the linear combination of i-th columns of (AB) with the i-th values in C_j.

$$\big((AB)C\big)_j = (AB)C_j = \begin{bmatrix} AB_1 & \cdots & AB_p \end{bmatrix} \begin{bmatrix} c_{1j} \\ \vdots \\ c_{pj} \end{bmatrix} = c_{1j}AB_1 + \cdots + c_{pj}AB_P$$

The j-th column of BC is equal BC_j, which is equal the linear column of the i-th columns of B with the i-th values in C_j:

$$\big(BC\big)_j = BC_j = c_{1j}B_1 + \cdots + c_{pj}B_p$$

The jth column of A(BC) is equal to the jth column of BC, $(BC)_j$ times A.

$$\big(A(BC)\big)_j = A\big(BC\big)_j = A\big(c_{1j}B_1 + \cdots + c_{pj}B_p\big) = c_1AB_1 + \cdots + c_{pj}AB_p = \big((AB)C\big)_j$$

Since the j-th column of (AB)C is equal to the j-th column of A(BC), it follows that

$$(AB)C = A(BC)$$

- distributivní zákony zřejmě platí (opět můžete ověřit pro obecné množiny A, B, C jako v případě asociativity).

⇨ $(M_n, +, \cdot)$ je okruh.

2. Nechť G je množina všech funkcí na $\langle 0, 1\rangle$, $+$ je operace sčítání funkcí a $\circ$ je operace skládání funkcí. Dokažte, že algebraická struktura $(G, +, \circ)$ není okruh.

Řešení:

Naším úkolem je nalézt takové funkce, které nějakým způsobem porušují podmínky platící pro okruh.

Zvolíme funkce $f_1 = x^2$, $f_2 = f_3 = 1$.

Ověříme, zda platí distributivní zákon $f_1 \circ (f_2 + f_3) = f_1 \circ f_2 + f_1 \circ f_3$:

$f_1 \circ (f_2 + f_3) = f_1(1+1) = (1+1)^2 = 4$.

$f_1 \circ f_2 + f_1 \circ f_3 = f_1(1) + f_1(1) = 1^2 + 1^2 = 2 \neq 4$.

⇨ jsou porušeny distributivní zákony, skutečně se nejedná o okruh. Navíc vidíme, že skládáním funkcí se snadno dostaneme mimo interval $\langle 0, 1\rangle$.

3. Doplňte níže uvedené tabulky tak, aby algebraická struktura $(A, +, \cdot)$ pro $A = \{a, b, c, d\}$ byl unitární okruh.

+	**a**	**b**	**c**	**d**
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	**a**	**b**	**c**	**d**
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

Řešení:

$(A, +)$ musí být abelovská grupa, tzn. pro první tabulku musí platit:

- symetrie podél hlavní diagonály => doplníme c do 1. sloupce ve 3. řádku
- v každém řádku i sloupečku se vyskytuje každý prvek právě jednou => doplníme d do 1. řádku, do 1. sloupce ve 4. řádku, do 3. sloupce ve 2. řádku, c do 4. sloupce ve 2. řádku
- musí obsahovat jednotku (kopíruje sloupeček i řádek) => prvek a
- musí být zachována asociativita (není nutné ověřovat)
- každý prvek musí mít k sobě inverzní prvek => zde je každý prvek inverzní sám k sobě, můžeme doplnit prvek a po celé hlavní diagonále
- zbylé prvky doplníme snadno podle předchozích pravidel:

$(A, \cdot)$ musí být monoid, tedy pro druhou tabulku musí platit:

- nulou monoidu bude prvek a („vynuluje“ celý řádek i sloupeček, doplníme)
- musí obsahovat jednotku => d („kopíruje“ celý řádek i sloupeček, doplníme)

Poslední dva prvky nalezneme následovně:

Zajímá nás výsledek operace $b \cdot c$. Díky distributivním zákonům musí platit např. rovnost $b \cdot (b + c) = b \cdot b + b \cdot c$.

Z předchozí tabulky víme, že $b + c = d$. Zároveň $b \cdot b = b$, tedy $b \cdot (b + c) = b \cdot d = b + b \cdot c$.

Jelikož $b \cdot d = b$, musí platit, že $b = b + b \cdot c$, tedy $b \cdot c = \mathbf{a}$.

Dále nás zajímá výsledek operace $c \cdot c$. Opět se nabízejí k využití distributivní zákony, konkrétně např. rovnost $c \cdot (b + c) = c \cdot b + c \cdot c$.

Jelikož $c \cdot b = a$ a zároveň $b + c = d$, pak $c \cdot (b + c) = c \cdot d = c$ a zároveň $c \cdot b + c \cdot c = a + c \cdot c$, tedy $c = a + c \cdot c \Rightarrow c \cdot c = \mathbf{c}$.

4. Ukažte, že ({a, b}, +, ·) je okruh. Je tento okruh i tělesem?

+	a	b
a	a	b
b	b	a

·	a	b
a	a	a
b	a	b

Řešení:

Je struktura okruhem?

({a, b}, +) musí být abelovská grupa:

– z tabulky plyne uzavřenost, existence jednotkového prvku a, inverzní prvky, komutativita. Měli bychom ověřit ještě asociativitu pro všechny možné trojice prvků:

$a+(a+b) = b = (a+a)+b$
$b+(a+b) = a = (b+a)+b$
$a+(a+a) = a = (a+a)+a$
$b+(b+b) = a = (b+b)+b$
$a+(b+b) = a = (a+b)+b$
$b+(b+a) = a = (b+b)+a$
$a+(b+a) = b = (a+b)+a$
$b+(a+a) = b = (b+a)+a$

⇨ jedná se o abelovskou grupu.

({a, b}, ·) musí být pologrupa:

- z tabulky plyne uzavřenost vůči operaci, měli bychom ověřit asociativitu. Víme ovšem, že prvek a je agresivní vůči násobení, tzn. všechny výrazy, v nichž se vyskytuje a, jsou rovny a (ověřte).
  Dále platí $b(b \cdot b) = (b \cdot b)b = b$. Struktura je tedy asociativní vůči operaci ·.

  Zbývá nám ověřit platnost distributivních zákonů. Jelikož operace · i + jsou komutativní, stačí nám ověřit pouze jeden z obou zákonů:
  $a(a+b) = a \cdot a + a \cdot b = a$
  $b(b+b) = b \cdot b + b \cdot b = a$

$a(a+a) = a \cdot a + a \cdot a = a$
$a(b+b) = a \cdot b + a \cdot b = a$
$b(a+a) = b \cdot a + b \cdot a = a$
$b(a+b) = b \cdot a + b \cdot b = b$

⇨ Distributivita je zachována. Struktura $(\{a, b\}, +, \cdot)$ je okruhem.

Aby byl okruh tělesem, musí být struktura $(\{a, b\} \setminus \{0\}, \cdot)$ grupa. Jelikož nulou okruhu je prvek a, vlastnosti ověřujeme pro množinu {b}. Víme ovšem, že těleso tvoří vždy minimálně dvouprvková množina.

⇨ Okruh není tělesem.

5. Nechť $+, \cdot$ jsou aritmetické operace na oboru $\mathbf{Z}$. Určete, které z následujících množin tvoří okruhy vzhledem k těmto operacím:

a) $\{2k, k \in \mathbf{Z}\}$
b) $\{2k+1, k \in \mathbf{Z}\}$

Řešení:

$\{2k, k \in \mathbf{Z}\}$ je množina sudých celých čísel.

Je $(2k, +)$ abelovská grupa?

- je uzavřená vůči + (součet dvou sudých čísel je vždy sudý)
- je asociativní díky asociativitě sčítání na Z
- jednotkový prvek je 0 (pro $x \in \mathbf{Z}$ platí $x+0 = x$, $0+x = x$)
- inverzním prvkem pro $x \in \mathbf{Z}$ je -x
- abelovská je díky komutativitě sčítání na $\mathbf{Z}$

⇨ Ano, $(2k, +)$ je abelovská grupa.

Je $(2k, \cdot)$ pologrupa?

- Je uzavřená vůči $\cdot$ (násobek dvou sudých čísel je vždy sudý)
- asociativní je díky asociativitě násobení na $\mathbf{Z}$

⇨ Ano, $(2k, \cdot)$ je pologrupa.

Distributivní zákony jsou zachovány (vyplývá z vlastností sčítání a násobení celých čísel).

⇨ Jedná se o okruh.

$\{2k+1, k \in \mathbf{Z}\}$ je množina všech lichých celých čísel.

Je $(2k+1, +)$ abelovská grupa?

- není uzavřená vůči +, např. $3+1 = 4$, 4 ovšem není liché číslo.

- také nemá jednotkový prvek, …

⇨ Nejedná se o abelovskou grupu, tedy struktura nemůže být okruhem.

6. Nalezněte takový okruh $(M, +, \cdot)$ a prvek $a \in M$, že $M \setminus \{a\}$ je podokruhem M.

Řešení:
Zvolit můžeme např. strukturu $(Z_2, \oplus, \otimes)$ jako okruh M, jako podokruh pak $(\mathbf{Z}_2 \setminus \{1\}, \oplus, \otimes)$.
Můžeme sestavit Cayleyho tabulky:

$(\mathbf{Z}_2, \oplus, \otimes)$:

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

$(\mathbf{Z}_2 \setminus \{1\}, \oplus, \otimes)$:

$\oplus$	0
0	0

$\otimes$	0
0	0

Vidíme, že množina $(\mathbf{Z}_2 \setminus \{1\}, \oplus, \otimes)$ splňuje vlastnosti okruhu a je skutečně podokruhem M. Jedná se o triviální podokruh, jelikož prvek 0 je nulou okruhu M.

7. Nechť P je podokruhem okruhu S a prvek $x \in P$ je netriviálním dělitelem nuly v S. Je nutně x dělitelem nuly i v P?

Řešení:
Nechť $S = (Z_6, \oplus, \otimes)$, $P = (\{0, 3\}, \oplus, \otimes)$, $x = 3$.
Sestavíme Cayleyho tabulky:

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	**0**	2	4
3	0	3	**0**	3	**0**	3

4	0	4	2	**0**	4	2
5	0	5	4	3	2	1

⇨ Vidíme, že 3 je triviálním dělitelem 0 v Z_6, jelikož $3 \otimes 2 = 0$, $3 \otimes 4 = 0$,…

$\otimes$	0	3
0	0	0
3	0	3

⇨ 3 není triviálním dělitelem 0 v $\{0, 3\}$: $3 \otimes 3 = 3$.

8. V okruhu $(\mathbf{Z}_{10}, \oplus, \otimes)$ definujeme podmnožiny $D_1 = \{0, 5\}$, $D_2 = \{0, 2, 4, 6, 8\}$. Zjistěte, zda jsou tyto množiny:

a) podokruhy $\mathbf{Z}_{10}$ vzhledem k operacím $\oplus$, $\otimes$
b) obory integrity

Vytvoříme Cayleyho tabulky pro D_1:

$\oplus$	0	5
0	0	5
5	5	0

- je uzavřená vůči $\oplus$, má jednotkový prvek 0, je asociativní díky asociativitě $\oplus$, obsahuje inverzní prvky (0 pro 0, 5 pro 5), je komutativní díky komutativitě $\oplus$

⇨ jedná se o abelovskou grupu.

$\otimes$	0	5
0	0	0
5	0	5

- je uzavřená, je asociativní díky asociativitě $\otimes$ => pologrupa
- distributivita je zachována (vyplývá z vlastností obou operací).

⇨ D_1 je okruh.

Je D_1 oborem integrity?

Okruh je komutativní díky komutativitě $\otimes$, jednotkou okruhu je 5, nemá žádné netriviální dělitele 0

⇨ D_1 je oborem integrity.

Vytvoříme Cayleyho tabulky pro D_2:

$\oplus$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

- je uzavřená vůči $\oplus$, asociativní díky asociativitě $\oplus$, jednotkový prvek je 0, má inverzní prvky (0 a 0, 2 a 8, 4 a 6), je komutativní

⇨ jedná se o abelovskou grupu

$\otimes$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

- je uzavřená vůči $\otimes$ i asociativní => jedná se o pologrupu
- distributivita je opět zachována

⇨ D_2 je okruh.

Je D_2 oborem integrity?

- neobsahuje netriviální dělitele 0, je komutativní, má jednotku (6).

⇨ D_2 je oborem integrity.

9. Je dána neprázdná množina A. Na její potenční množině ExpA jsou definovány operace + a · následujícím způsobem:

$$X+Y = (X\setminus Y) \cup (Y\setminus X)$$
$$X\cdot Y = X \cap Y$$

Zjistěte, zda (ExpA, +, ·) je okruh. Pokud ano, co je nulou tohoto okruhu? Má nějaké dělitele nuly?

Řešení:

Zkusíme si vytvořit Cayleyovy tabulky operací např. pro množinu A = {a, b}, tzn. ExpA = {∅, {a}, {b}, {a, b}}. Poté zobecníme získané poznatky.

+	∅	{a}	{b}	{a, b}
∅	∅	{a}	{b}	{a, b}
{a}	{a}	∅	{a, b}	{b}
{b}	{b}	{a, b}	∅	{a}
{a, b}	{a, b}	{b}	{a}	∅

- množina je zjevně uzavřená vůči operaci +
- je asociativní díky asociativitě operace ∪
- jednotkovým prvkem je ∅ (kopíruje řádek i sloupec)
- obsahuje inverzní prvky: {a} pro {a}, {b} pro {b}, {a, b} pro {a, b}, ∅ pro ∅ - každý prvek je inverzní sám k sobě.
- je komutativní (tabulka je symetrická podél hlavní diagonály)

⇨ jedná se o abelovskou grupu.

·	∅	{a}	{b}	{a, b}
∅	∅	∅	∅	∅
{a}	∅	{a}	∅	{a}
{b}	∅	∅	{b}	{b}
{a, b}	∅	{a}	{b}	{a, b}

- množina je uzavřená vůči operaci · a je asociativní díky asociativitě operace ∩, tedy se jedná o pologrupu.
- ověříme distributivní zákony (opět stačí ověřit pouze jeden):
  A(B+C) = A ∩ ((B\C) ∪ (C\B)) = (A ∩ (B\C)) ∪ (A ∩ (C\B)) = ((A ∩ B) \ (A ∩ C)) ∪ ((A∩C) \ (A∩B))
  AB+AC = ((A∩B) \ (A∩C)) ∪ ((A∩C) \ (A∩B))

⇨ distributivita je zachována. Jedná se o okruh, jehož nulou je ∅.

Netriviální dělitelé nuly jsou všechny podmnožiny množiny ExpA krom A, jelikož pro libovolnou podmnožinu X ⊂ A platí X ∩ (A \ X) = ∅.

10. Na oboru $\mathbf{R}$ jsou definovány operace $\oplus$, $\otimes$ pro $a, b \in \mathbf{R}$ jako:

$$a \oplus b = a+b+1$$
$$a \otimes b = a+b+ab$$

Ověřte, zda $(\mathbf{R}, \oplus, \otimes)$ tvoří okruh.

Řešení:

Je $(\mathbf{R}, \oplus)$ abelovská grupa?

- je zjevně uzavřená vůči $\oplus$
- aby byla asociativní, musí platit $(a \oplus b) \oplus c = a \oplus (b \oplus c)$:
  $(a+b+1)+c+1 = a+(b+c+1)+1 = a+b+c+2 \Rightarrow$ asociativita platí
- jednotkový prvek bude -1, jelikož $a \oplus -1 = a+(-1)+1=a$.
- inverzní prvek vůči a bude –a-2: $a \oplus (-a-2) = a+(-a-2)+1=-1$
- komutativní je, jelikož $a \oplus b=b \oplus a=a+b+1 = b+a+1$

⇨ $(\mathbf{R}, \oplus)$ je abelovská grupa.

Je $(\mathbf{R}, \otimes)$ pologrupa?

- je uzavřená vůči $\otimes$ (výsledkem bude opět reálné číslo)
- ověříme asociativitu, tzn. zda platí $(a \otimes b) \otimes c = a \otimes (b \otimes c)$:
- $(a \otimes b) \otimes c = (a+b+ab)+c+(a+b+ab)c = a+b+ab+c+ac+bc+abc$
- $a \otimes (b \otimes c) = a+(b+c+bc)+a(b+c+bc) = a+b+c+bc+ab+ac+abc$

⇨ asociativita je zachována, $(\mathbf{R}, \otimes)$ je tedy pologrupa.

Ověříme distributivní zákony (díky komutativitě obou operací stačí ověřit pouze jeden z nich):

$a \otimes (b \oplus c) = a \otimes (b+c+1) = a+(b+c+1)+a(b+c+1)=a+b+c+1+ab+ac+a$

$a \otimes b \oplus a \otimes c = (a+b+ab) \oplus (a+c+ac) = a+b+ab+a+c+ac+1$

⇨ distributivita je zachována, $(\mathbf{R}, \oplus, \otimes)$ je tedy skutečně okruh.