Úlohy 8

Na případné chyby mě prosím upozorněte. Děkuji.

1. Je dána množina $M = \{a, b\}$ a její potence $\text{Pot}(M)$. Rozhodněte, zda uspořádaná dvojice $(\text{Pot}(M), \cap)$ je algebraickou strukturou. Pokud ano, určete, o jakou strukturu se jedná.

   Řešení:

   Nejprve určíme potenční množinu $\text{Pot}(M)$ pro $M = \{a, b\}$:

   $$\text{Pot}(M) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

   Tedy potenční množina obsahuje čtyři podmnožiny.

   Zkoumáme, zda je struktura $(\text{Pot}(M), \cap)$ algebraickou strukturou.

   Uvažujeme operaci průniku $(\cap)$, která se aplikuje na podmnožiny M. Zkoumejme, jaké $(\text{Pot}(M), \cap)$ splňuje vlastnosti algebraické struktury:

   (a) *Uzavřenost*: operace průniku dvou podmnožin množiny M vždy vrátí podmnožinu M, což znamená, že výsledek operace $A \cap B$ pro $A, B \in \text{Pot}(M)$ je vždy v $\text{Pot}(M)$.

   (b) *Asociativita*: operace je asociativní, protože pro všechny $A, B, C \in \text{Pot}(M)$ platí:

   $$(A \cap B) \cap C = A \cap (B \cap C)$$

   (c) *Existence neutrálního prvku*: neutrálním prvkem operace průniku je množina M sama, což v našem případě je $\{a, b\}$. Platí, že pro všechny $A \in \text{Pot}(M)$ je:

   $$A \cap \{a, b\} = A$$

   Tedy neutrální prvek existuje.

   (d) *Komutativita*: průnik dvou množin je komutativní, což znamená, že pro všechny $A, B \in \text{Pot}(M)$ platí:

   $$A \cap B = B \cap A$$

   (e) *Existence inverzního prvku*: u průniku neexistuje inverzní prvek, který by z podmnožiny udělal neutrální prvek $\{a, b\}$. Inverzní prvek tedy neexistuje.

   Struktura $(\text{Pot}(M), \cap)$ je komutativní monoid, protože splňuje uzavřenost, asociativitu, komutativitu a má neutrální prvek. Nejedná se však o grupu, protože nemá inverzní prvek.

2. Je dána množina $M = \{a, b\}$ a její potence $\text{Pot}(M)$. Rozhodněte, zda $(\text{Pot}(M), \cup)$ je algebraickou strukturou. Pokud ano, určete, o jakou strukturu se jedná.

   Nápověda: Jedná se o komutativní monoid.

3. Rozhodněte, zda $(M, \circ)$ je algebraickou strukturou. Pokud ano, určete, o jakou strukturu se jedná.

   (a) $M = \mathbb{N}$ a $x \circ y = (x + y)x$

(b) $M = \mathbb{R}$ a $x \circ y = (x+y)x$

(c) $M = \mathbb{N}$ a $x \circ y = 0$

(d) $M = \mathbb{R}$ a $x \circ y = x$

(e) $M = \mathbb{Q}$ a $x \circ y = \frac{x+y}{2}$

(f) $M = \mathbb{R}$ a $x \circ y = \frac{x+y}{2}$

(g) M jsou kladná racionální čísla a $x \circ y = \sqrt{xy}$

(h) M jsou kladná reálná čísla a $x \circ y = \sqrt{xy}$

Řešení:

(a) $M = \mathbb{N}$ a $x \circ y = (x+y)x$

Uzavřenost: Pro $x, y \in \mathbb{N}$ platí, že $(x+y)x \in \mathbb{N}$, protože součet přirozených čísel je zase přirozené číslo a součin přirozených čísel je rovněž přirozené číslo. Množina je vůči operaci uzavřená.

Asociativita:

$$(x \circ y) \circ z = ((x+y)x) \circ z = (((x+y)x + z)(x+y)x),$$

$$x \circ (y \circ z) = x \circ ((y+z)y) = (x + (y+z)y)x.$$

Výrazy nejsou stejné obecně pro všechna $x, y \in \mathbb{N}$, operace není asociativní.

Závěr: Je to grupoid.

(b) $M = \mathbb{R}$ a $x \circ y = (x+y)x$

Uzavřenost: Pro $x, y \in \mathbb{R}$ platí, že $(x+y)x \in \mathbb{R}$, protože součet reálných čísel je reálné číslo a součin reálných čísel je rovněž reálné číslo. Množina je tedy vůči operaci uzavřená.

Asociativita: Viz předchozí, operace není asociativní.

Závěr: Je to grupoid.

(c) $M = \mathbb{N}$ a $x \circ y = 0$

Uzavřenost: $x \circ y = 0$ a $0 \in \mathbb{N}$, tedy množina je uzavřená vůči operaci $\circ$.

Asociativita:

$$(x \circ y) \circ z = 0 \circ z = 0, \quad x \circ (y \circ z) = x \circ 0 = 0.$$

Operace je asociativní.

Neutrální prvek: Nenajdeme, protože by muselo platit

$$(\exists e)(\forall y) e \circ y = y \circ e = y.$$

A to nebude platit pro $y \neq 0$, protože výsledek operace je vždy 0. A my potřebujeme, aby to platilo pro všechna y.

Závěr: Jedná se o pologrupu.

(d) $M = \mathbb{R}$ a $x \circ y = x$

Uzavřenost: Pro $x, y \in \mathbb{R}$ je $x \circ y = x$ a $x \in \mathbb{R}$, množina je vůči operaci uzavřená.

Asociativita:

$$(x \circ y) \circ z = x \circ z = x, \quad x \circ (y \circ z) = x \circ y = x.$$

Operace je asociativní.
Neutrální prvek: Nenajdeme. Muselo by platit

$$(\exists e)(\forall y) e \circ y = y \circ e = y.$$

ale pro každý prvek e

$$e \circ y = e \quad y \circ e = y$$

Z toho by vyplývalo $y = e$, jenže my potřebujeme, aby to platilo pro každé y, a to neplatí.
Závěr: Jedná se o pologrupu.

(e) $M = \mathbb{Q}$ a $x \circ y = \frac{x+y}{2}$
Uzavřenost: Pro $x, y \in \mathbb{Q}$ je $x \circ y = \frac{x+y}{2}$. Součet dvou racionálních čísel je zase racionální číslo. Podíl racionálního čísla a 2 je také racionální číslo. Tedy množina je vůči operaci uzavřená.
Asociativita:

$$(x \circ y) \circ z = \frac{x + y + 2z}{4}, \quad x \circ (y \circ z) = \frac{2x + y + z}{4}.$$

Operace není asociativní.
Závěr: Je to grupoid.

(f) $M = \mathbb{R}$ a $x \circ y = \frac{x+y}{2}$
Uzavřenost: Pro $x, y \in \mathbb{R}$ je $x \circ y = \frac{x+y}{2}$, součet dvou reálných čísel je reálné čísel, podíl reálného čísla a 2 je také reálné číslo. Množina je vůči operaci uzavřená.
Asociativita: není asociativní, viz předchozí.
Závěr: Je to grupoid.

(g) M jsou kladná racionální čísla a $x \circ y = \sqrt{xy}$
Uzavřenost: $\sqrt{xy}$ nemusí být racionální, např. pro $x = 1$ a $y = 2$, máme $x \circ y = \sqrt{2}$, a to není racionální číslo. Množina $\mathbb{Q}$ není vůči operaci uzavřená.
Závěr: Nejedná se o žádnou algebraickou strukturu.

(h) M jsou kladná reálná čísla a $x \circ y = \sqrt{xy}$
Uzavřenost: Pro $x, y \in \mathbb{R}^+$ je $\sqrt{xy}$ vždy reálné číslo. Množina je vůči operaci uzavřená.
Asociativita:

$$(x \circ y) \circ z = \sqrt{\sqrt{xy}z}, \quad x \circ (y \circ z) = \sqrt{x\sqrt{yz}}.$$

Operace není asociativní.
Závěr: Jedná se o grupoid.

4. Rozhodněte, zda $(M, \circ)$ je algebraickou strukturou. Pokud ano, určete, o jakou strukturu se jedná.

(a) $M = \mathbb{N}$ a $x \circ y = x - y$

(b) $M = \mathbb{R}$ a $x \circ y = x^2 y$

(c) $M = \mathbb{N}$ a $x \circ y = 3$

(d) $M = \mathbb{R}$ a $x \circ y = y$

(e) $M = \mathbb{Q}$ a $x \circ y = \pi$

(f) $M = \mathbb{R}$ a $x \circ y = \pi$

(g) M jsou kladná racionální čísla a $x \circ y = \sqrt{x}$

(h) M jsou kladná reálná čísla a $x \circ y = \sqrt{y}$

5. Sestavte Cayleyho tabulku operace sčítání modulo 4. O jakou algebraickou strukturu se jedná? Ověřte příslušné vlastnosti.

6. Doplňte Cayleyho tabulku tak, aby struktura $(M, \circ)$ byla komutativní grupa.

$\circ$	m	n	p	q
m	q	p	m	n
n				
p	m			
q	n			p

Řešení:

(a) *Komutativita*

Protože se jedná o komutativní grupu, musí platit, že $a \circ b = b \circ a$ pro všechny $a, b \in M$. To znamená, že tabulka musí být symetrická. Využijeme toho k doplnění prázdných polí tak, aby se hodnoty na pozicích (i, j) a (j, i) shodovaly.

(b) *Neutrální prvek*

Neutrální prvek e je takový, že $e \circ a = a \circ e = a$ pro všechna $a \in M$. Z tabulky můžeme vidět, že prvek p jako jediný může plnit tuto roli a doplníme:

- $m \circ p = m$, $n \circ p = n$, $p \circ p = p$, $q \circ p = q$.

Doplníme i symetricky, protože je komutativní.

(c) *Inverzní prvky*

Každý prvek v grupě musí mít inverzní prvek, tj. prvek a^{-1}, pro který platí $a \circ a^{-1} = e$, kde e je neutrální prvek. Z tabulky můžeme odvodit inverzní prvky následovně:
- Pro prvek m je inverzním prvkem n, protože $m \circ n = p$ (a p je neutrální prvek).
- Pro prvek n je inverzním prvkem m, protože $n \circ m = p$.
- Pro prvek q je jeho inverzním prvkem q, protože $q \circ q = p$.
- Pro prvek p je inverzním prvkem p (neutrální prvek je svůj vlastní inverzní prvek).

Doplníme také symetricky.

(d) *Finální podoba tabulky*

Nyní můžeme vyplnit zbývající hodnoty tak, aby každý prvek byl v každém řádku a v každém sloupci právě jednou, čímž je splněna asociativita. Asociativitu je možné v konečné množině dokázat pouze skutečným ověřením pro všechny uspořádané trojice prvků (v tomto případě variace trojic s opakováním ze čtyř prvků, tj. 4^3). Pro naše účely však zkusíme, zda asociativita platí třeba pro dvě uspořádané trojice, a pokud ano, pak to budeme v tuto chvíli považovat za splněné.

	m	n	p	q
m	q	p	m	n
n	p	q	n	m
p	m	n	p	q
q	n	m	q	p

$$(q \circ p) \circ m = q \circ (p \circ m) \text{... obě strany jsou rovny } n$$

$$(m \circ n) \circ q = m \circ (n \circ q) \text{... obě strany jsou rovny } q$$

Tedy předpokládáme, že asociativita je splněna.

(e) *Závěr*

Tato tabulka splňuje všechny podmínky pro komutativní grupu. Je komutativní, protože tabulka je symetrická. Obsahuje neutrální prvek p. Každý prvek má inverzní prvek. Je asociativní.

7. Doplňte Cayleyho tabulku tak, aby struktura $(M, \circ)$ byla komutativní grupa, kde $M = \{a, b, c, d\}$.

$\circ$	a	b	c	d
a	a	b	c	d
b	b		a	
c	c			
d	d			

8. Doplňte Cayleyho tabulku tak, aby struktura $(N, \cdot)$ byla komutativní grupa na množině $N = \{e, f, g, h\}$.

$\cdot$	e	f	g	h
e	e	f		
f	f	e		
g			e	
h				e

9. Vyplňte Cayleyho tabulku tak, aby struktura $(A, *)$ byla komutativní monoid, ale nikoli grupa. $A = \{a, b\}$.

$*$	a	b
a		
b		

Řešení:

$*$	a	b
a	a	b
b	b	b

Tato struktura je asociativní protože

$$\begin{aligned}
(a*a)*a &= a = & a*(a*a) \\
(b*b)*b &= b = & b*(b*b) \\
(a*b)*b &= b = & a*(b*b) \\
(b*a)*b &= b = & b*(a*b) \\
(b*b)*a &= b = & b*(b*a) \\
(b*a)*a &= b = & b*(a*a) \\
(a*b)*a &= b = & a*(b*a) \\
(a*a)*b &= b = & a*(a*b)
\end{aligned}$$

Má neutrální prvek a, protože

$$\begin{aligned}
a*a &= a = & a*a \\
b*a &= b = & a*b
\end{aligned}$$

Je komutativní, protože Cayleyho tabulka je symetrická.

Nemá inverzní prvek, protože prvek b nemá k sobě inverzní prvek:

$$\begin{aligned}
b*a &= b \\
b*b &= b
\end{aligned}$$

Ve struktuře není žádný prvek, po jehož vynásobením s b bychom získali a.

Tedy je to komutativní monoid, ale není to grupa.

10. Je $(M,*)$, $M = \{a,b,c,d\}$ zadaná Cayleyho tabulkou algebraickou strukturou? Je komutativní?

$*$	a	b	c	d
a	0	0	0	1
b	0	0	1	0
c	0	1	0	0
d	1	0	0	0

11. Je $(M,+)$, $M = \{0,1,2\}$ zadaná Cayleyho tabulkou algebraickou strukturou? Je komutativní?

$+$	0	1	2
0	0	0	0
1	0	0	1
2	0	1	0

12. Je dán obdélník $ABCD$. Zákrytovým pohybem obdélníku budeme rozumět takový pohyb, který převede daný obdélník na sebe sama. Mějme dánu množinu M, která obsahuje všechny zákrytové pohyby obdélníku (nějak si je označte) a dále operaci skládání zákrytových pohybů $\square$. Určete, o jakou strukturu se jedná.

Nápověda: Zákrytové pohyby obdélníku jsou čtyři. Jedná se o komutativní grupu.

13. Je dána množina $M = \{a, b\}$ a její potence $\mathrm{Pot}(M)$. Rozhodněte a zdůvodněte, zda uspořádaná trojice $(\mathrm{Pot}\, M, \cup, \cap)$ je okruhem.

14. Uveďte příklad grupy s nekonečnou množinou jako nosičem, uveďte, jaké vlastnosti musí splňovat, a podrobně zdůvodněte, proč je splňuje.

15. Uveďte příklad konečného oboru integrity, uveďte, jaké vlastnosti musí splňovat, a podrobně zdůvodněte, proč je splňuje.

    Nápověda: Příklad konečného oboru integrity je například

$$(\mathbb{N}/\mod{2}, +_{\mod (2)}, \cdot_{\mod (2)}).$$

$+_{\mod (2)}$	0	1
0	0	1
1	1	0

$\cdot_{\mod (2)}$	0	1
0	0	0
1	0	1

16. Uveďte příklad konečného tělesa, uveďte, jaké vlastnosti musí splňovat, a podrobně zdůvodněte, proč je splňuje.

17. Uveďte příklad tělesa s nekonečnou množinou jako nosičem, uveďte, jaké vlastnosti musí splňovat, a podrobně zdůvodněte, proč je splňuje.

18. Je $(\mathbb{N}/\mod{6}, +_{\mod (6)}, \cdot_{\mod (6)})$ okruhem? Je oborem integrity? Je tělesem? Odpověď řádně zdůvodněte.

19. Uvažujme množinu Gaussových celých čísel. Gaussovo celé číslo je v teorii čísel takové komplexní číslo, jehož reálnou i imaginární složku tvoří celá čísla. Formálně

$$\mathbb{Z}[i] = \{a + bi; a \in \mathbb{Z}, b \in \mathbb{Z}\}$$

    Uvažujme obvyklé sčítání a násobení komplexních čísel.

$$a + b = (a_1 + ia_2) + (b_1 + ib_2) = (a_1 + b_1) + i(a_2 + b_2)$$

$$a \cdot b = (a_1 + ia_2) \cdot (b_1 + ib_2) = (a_1b_1 - a_2b_2) + i(a_1b_2 + a_2b_1)$$

    Rozhodněte a zdůvodněte, jakou strukturu tvoří uspořádaná trojice $(\mathbb{Z}[i], +, \cdot)$

    Nápověda: Jedná se o obor integrity.