Příklady na procvičení z Lineární algebry 1 (ZS 2020/2021): (5) Grupy a tělesa

Cv. 1. Zjistěte, zda je grupou:

(a) $(\mathbb{Q}, \cdot)$,

(b) $(\mathbb{Q}, -)$,

(c) $(\mathbb{Q} \setminus \{0\}, \circ)$, kde $a \circ b = |ab|$ pro všechna $a, b \in \mathbb{Q}$,

(d) $(\mathbb{Q}, \circ)$, kde $a \circ b = \frac{a+b}{2}$ pro všechna $a, b \in \mathbb{Q}$,

(e) $(\mathbb{Q}, \circ)$, kde $a \circ b = a + b + 3$ pro všechna $a, b \in \mathbb{Q}$,

(f) $(\mathcal{F}, +)$, tj. množina $\mathcal{F}$ všech reálný funkcí jedné proměnné s operace sčítání funkcí,

(g) množina rotací v $\mathbb{R}^2$ kolem počátku s operací skládání zobrazení,

(h) množina posunutí v $\mathbb{R}^2$ s operací skládání zobrazení.

Řešení:

(a) $(\mathbb{Q}, \cdot)$ není grupou, protože neexistuje inverzní prvek k 0.

(b) $(\mathbb{Q}, -)$ není grupou, protože rozdíl racionálních čísel není asociativní. Například $(8-6)-1 = 1 \neq 3 = 8-(6-1)$.

(c) $(\mathbb{Q} \setminus \{0\}, \circ)$, kde $a \circ b = |ab|$ pro všechna $a, b \in \mathbb{Q}$ není grupou, protože není zaručena existence neutrálního prvku. Pro libovolné $a < 0$ je $a \circ e = |ae| > 0 > a$ pro všechna e, tudíž žádné e nemůže splňovat definici neutrálního prvku pro záporná a.

(d) $(\mathbb{Q}, \circ)$, kde $a \circ b = \frac{a+b}{2}$ pro všechna $a, b \in \mathbb{Q}$ není grupou, protože aritmetický průměr čísel není asociativní. Například pro $a = 1, b = 5, c = 7$ máme $a \circ (b \circ c) = \frac{1}{2}\left(1 + \frac{5+7}{2}\right) = 3.5 \neq 5 = \frac{1}{2}\left(\frac{1+5}{2} + 7\right) = (a \circ b) \circ c$.

(e) $(\mathbb{Q}, \circ)$, kde $a \circ b = a + b + 3$ pro všechna $a, b \in \mathbb{Q}$, je grupou. Asociativita platí z asociativity sčítání nad $\mathbb{Q}$. Neutrální prvek je $e = -3$, protože pro každé $a \in \mathbb{Q}$ platí

$$a \circ e = a + (-3) + 3 = a = (-3) + a + 3 = e \circ a\ .$$

Konečně, inverzní prvek pro každé $a \in \mathbb{Q}$ je $b = -a - 6$, protože

$$a \circ b = a + (-a-6) + 3 = -3 = e = -3 = (-a-6) + a + 3 = b \circ a\ .$$

(f) $(\mathcal{F}, +)$ je grupou. Asociativita plyne z definice součtu funkcí a asociativity sčítání nad $\mathbb{R}$. Pro každé $f, g, h \in \mathcal{F}$ a $x \in \mathbb{R}$ platí $f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)$. Neutrální prvek je identicky nulová funkce $e(x) = 0$ pro všechna $x \in \mathbb{R}$. Inverzní prvek pro každou $f \in \mathcal{F}$ je funkce $-f$.

(g) Je grupou. Asociativita plyne z asociativity skládání zobrazení. Neutrálním prvkem je například rotace o 360 stupňů. Inverzním prvkem k rotaci o úhel α je rotace o úhel α v opačném směru.

(h) Je grupou. Asociativita plyne z asociativity skládání zobrazení. Neutrálním prvkem je identické zobrazení $e((x_1, x_2)^T) = (x_1, x_2)^T$ (tj. posunutí vektorem $(0, 0)^T$) a inverzím prvkem ke každému posunutí $t((x_1, x_2)^T) = (x_1, x_2)^T + (a, b)^T$ je posunutí $t^{-1}((x_1, x_2)^T) = (x_1, x_2)^T - (a, b)^T$.

Cv. 2. Vyplňte tabulku pro binární operaci $\circ$ na $\mathbb{G}$ tak aby $(\mathbb{G}, \circ)$ byla grupou s neutrálním prvkem 0. Zdůvodněte.

(a)

$\circ$	0	1
0		
1		

(b)

$\circ$	0	1	2
0			
1			
2			

(c)

$\circ$	0
0	

(d)

$\circ$	0	1	2	3
0				
1		0		
2				
3				

Řešení:

První tři tabulky jsou určeny jednoznačně. Fakt, že 0 je neutrálním prvkem pro $\circ$ určuje první řádek i sloupec tabulky. Existence levého i pravého inverzu omezuje pozice 0 na diagonále nebo symetricky podle diagonály. Asociativita vynutí zbylé pozice. Dostáváme:

(a)

$\circ$	0	1
0	0	1
1	1	0

- aditivní grupu modulo 2,

(b)

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

– aditivní grupu modulo 3,

(c)

$\circ$	0
0	0

– triviální grupu,

(d) například

$\circ$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

– Kleinovu grupu, tj. grupu symetrií obdélníka.

Cv. 3. Nechť $(\mathbb{G}, \circ)$ je grupa a $x \in \mathbb{G}$. Rozhodněte, zda $(\mathbb{G}, *)$ je grupou s operací definovanou $a * b = a \circ x \circ b$ pro všechna $a, b \in \mathbb{G}$.

Řešení:
Ověříme definici grupy. Nová operace je asociativní jelikož $\circ$ je asociativní. Pro všechna $a, b, c, x \in \mathbb{G}$ platí:

$$a * (b * c) = a \circ x \circ (b \circ x \circ c) = (a \circ x \circ b) \circ x \circ c = (a * b) * c \ ,$$

kde jsme prostřední rovnost dostali díky asociativitě $\circ$ na $\mathbb{G}$ aplikované na prvky $\alpha = a \circ x, \beta = b$ a $\gamma = x \circ c$ grupy $\mathbb{G}$.

Označme E neutrální prvek v $(\mathbb{G}, \circ)$. Neutrálním prvkem $(\mathbb{G}, *)$ je inverzní prvek x vzhledem k $\circ$, tj. $e = x^{-1}$ vzhledem k $\circ$. Ověříme pro všechna $a, x \in \mathbb{G}$:

$$e * a = x^{-1} \circ x \circ a = E \circ a = a = a \circ E = a \circ x \circ x^{-1} = a * e \ .$$

Podobně, inverzní prvek pro každé $a \in \mathbb{G}$ v grupě $\mathbb{G}$ je $b = x^{-1} \circ a^{-1} \circ x^{-1}$, kde a^{-1} je inverzní prvek k a v grupě $(\mathbb{G}, \circ)$. Ověříme pro všechna $a, x \in \mathbb{G}$:

$$\begin{aligned} a * b &= a \circ x \circ x^{-1} \circ a^{-1} \circ x^{-1} = a \circ E \circ a^{-1} \circ x^{-1} = a \circ a^{-1} \circ x^{-1} = E \circ x^{-1} \\ &= x^{-1} = e \\ &= x^{-1} \circ E = x^{-1} \circ a^{-1} \circ a = x^{-1} \circ a^{-1} \circ E \circ a = x^{-1} \circ a^{-1} \circ x^{-1} \circ x \circ a \\ &= b * a \ . \end{aligned}$$

Cv. 4. Rozhodněte a zdůvodněte, zda je Abelovou (komutativní) grupou:

(a) množina $\{\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right) \mid z \in \mathbb{Z}\}$ s maticovým součinem,

(b) množina $\{\left(\begin{smallmatrix} a & a \\ a & a \end{smallmatrix}\right) \mid a \in \mathbb{R} \setminus \{0\}\}$ s maticovým součinem.

Řešení:

(a) Ano. Nejdříve ukážeme, že maticový součin je uzavřený pro danou množinu. Pro všechna $a, b \in \mathbb{Z}$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + b \\ 0 & 1 \end{pmatrix} \ , \tag{1}$$

což je matice náležející do zadané množiny ($z = a + b \in \mathbb{Z}$ pro všechna $a, b \in \mathbb{Z}$).

Asociativita maticového součinu na dané množině plyne z asociativity maticového součinu pro obecné čtvercové matice stejných rozměrů.

Neutrálním prvkem je jednotková matice řádu dva, jež patří do zadané množiny ($z = 0 \in \mathbb{Z}$).

Konečně, inverzním prvkem pro libovolnou matici $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ je celočíselná matice $\left(\begin{smallmatrix} 1 & -z \\ 0 & 1 \end{smallmatrix}\right)$, což plyne z rovnosti (1).

Zadaná množina matic spolu s maticovým součinem tvoří grupu. Zbývá ověřit, zda je maticový součin pro tyto matice komutativní. Komutativita maticového součinu plyne z rovnosti (1) a komutativity sčítání nad $\mathbb{Z}$. Ověřili jsme tedy, že se jedná o Abelovskou grupu.

(b) Ano. Nejdříve ukážeme, že maticový součin je uzavřený pro danou množinu. Pro všechna $a, b \in \mathbb{R} \setminus \{0\}$

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix}, \tag{2}$$

což je matice náležející do zadané množiny ($2ab \neq 0$ pro všechna $a, b \in \mathbb{R} \setminus \{0\}$).

Asociativita maticového součinu na dané množině plyne z asociativity maticového součinu pro obecné čtvercové matice.

Neutrálním prvkem je matice $\frac{1}{2}\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, jež patří do zadané množiny.

Konečně, pro všechna $a \in \mathbb{R} \setminus \{0\}$ je inverzním prvkem pro matici $\left(\begin{smallmatrix} a & a \\ a & a \end{smallmatrix}\right)$ matice $\frac{1}{4a}\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, což plyne z rovnosti (2) (všimněte si, že inverzní prvek je definován, protože $a \neq 0$).

Zadaná množina matic spolu s maticovým součinem tvoří grupu. Zbývá ověřit, zda je maticový součin pro tyto matice komutativní. Komutativita maticového součinu plyne z rovnosti (2) a komutativity součinu nad $\mathbb{R}$. Ověřili jsme tedy, že se jedná o Abelovskou grupu.

Cv. 5. Vyjádřete jako prvky daného tělesa výrazy:

(a) $((2^{-1} + 1)4)^{-1}, 4/3$ v $\mathbb{Z}_5$,

(b) $6 + 7, -7, 6 \cdot 7, 7^{-1}, 6/7$ v $\mathbb{Z}_{11}$.

Řešení:

(a) Těleso $\mathbb{Z}_5$ je definováno jako množina všech zbytků v $\mathbb{Z}$ po dělení 5 spolu s operacemi součtu a součinu modulo 5. Sčítat modulo 5 lze jednoduše. Pro ostatní výpočty v $\mathbb{Z}_5$ nám poslouží tabulka pro operaci součinu modulo 5.

$\mathbb{Z}_5, \cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Všimněte si, že z tabulky je vidět, že množina $\mathbb{Z}_5 \setminus \{0\} = \{1, 2, 3, 4\}$ se součinem modulo 5 tvoří grupu – takzvanou multiplikativní grupu modulo 5. Toto není překvapivé, protože těleso je definováno jako množina $\mathbb{T}$ s operacemi sčítání $+$ a násobení $\cdot$ na $\mathbb{T}$, takovými že $(\mathbb{T}, +)$ je grupa s neutrálním prvkem 0 a $(\mathbb{T} \setminus \{0\}, \cdot)$ je také grupa.

Nyní můžeme vyhodnotit zadané výrazy v $\mathbb{Z}_5$, kde při výpočtu nalezneme multiplikativní inverz k libovolnému $a \in \mathbb{Z}_5 \setminus \{0\}$ v tabulce tak, že v řádku s a najdeme hodnotu 1 a index b odpovídajícího sloupce musí být hledaný multiplikativní inverz a^{-1}, protože $a \cdot b = 1$ v $\mathbb{Z}_5$. Dostáváme:

$$((2^{-1}+1)4)^{-1} = ((3+1)4)^{-1} = (4 \cdot 4)^{-1} = (1)^{-1} = 1 \text{ v } \mathbb{Z}_5$$

a

$$4/3 = 4 \cdot 3^{-1} = 4 \cdot 2 = 3 \text{ v } \mathbb{Z}_5.$$

(b) Postupujeme podobně jako pro $\mathbb{Z}_5$, ale nebudeme konstruovat celou tabulku pro součin v $\mathbb{Z}_{11}$. Dostáváme:

$$\begin{aligned} 6+7 &= 6+7 \pmod{11} = 2 \text{ v } \mathbb{Z}_{11}, \\ -7 &= 11-7 \pmod{11} = 4 \text{ v } \mathbb{Z}_{11}. \\ 6 \cdot 7 &= 6 \cdot 7 \pmod{11} = 42 \pmod{11} = 9 \text{ v } \mathbb{Z}_{11}. \end{aligned}$$

Při hledání multiplikativního inverzu k prvku 7 můžeme postupovat jako při výpočtu řádku odpovídajícího 7 v tabulce pro součin v $\mathbb{Z}_{11}$. Výpočet zastavíme v momentě, kdy uvidíme 1:

$$\begin{aligned} 7 \cdot 1 &= 7, \\ 7 \cdot 2 &= 3, \\ 7 \cdot 3 &= 10, \\ 7 \cdot 4 &= 6, \\ 7 \cdot 5 &= 2, \\ 7 \cdot 6 &= 9, \\ 7 \cdot 7 &= 5, \\ 7 \cdot 8 &= 1. \end{aligned}$$

Vidíme, že

$$7^{-1} = 8 \text{ v } \mathbb{Z}_{11}.$$

Tuto hodnotu využijeme i při posledním výpočtu:

$$6/7 = 6 \cdot 7^{-1} = 6 \cdot 8 = 48 \pmod{11} = 4 \text{ v } \mathbb{Z}_{11}.$$

Cv. 6. Nad $\mathbb{Z}_5$ najděte množinu všech řešení soustavy rovnic

$$\begin{aligned} 3x + 2y + z &= 1 \\ 4x + y + 3z &= 3 \end{aligned}$$

a spočítejte její mohutnost.

Řešení:

Postupujeme podobně jako pro soustavy rovnic nad $\mathbb{R}$. Využijeme toho, že eliminovat prvky pod pivotem můžeme přičtením vhodného násobku řádku s pivotem. Přičtením 2-násobku prvního řádku k druhému dostáváme

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 4 & 1 & 3 & 3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Za volné proměnné zvolíme parametry $y, z \in \mathbb{Z}_5$ a vyjádříme

$$x = 3^{-1}(1 - 2y - z) = 2(1 + 3y + 4z) = 2 + y + 3z \ .$$

Množina všech řešení dané soustavy je tedy

$$\{(2,0,0)^T + y(1,1,0)^T + z(3,0,1)^T \mid y, z \in \mathbb{Z}_5\} \ .$$

Máme $25 = 5 \cdot 5$ různých voleb parametrů y a z a mohutnost množiny řešení je tedy 25.

Cv. 7. Nalezněte multiplikativní inverzy 9^{-1} a 12^{-1} v $\mathbb{Z}_{31}$.

Řešení:
Mohli bychom postupovat stejně jako pro $\mathbb{Z}_{11}$, ale výpočet by mohl trvat 31 kroků pro zkonstruování celého řádku odpovídajícího prvku 9 v tabulce pro součin v $\mathbb{Z}_{31}$. Efektivní metodou je použití rozšířeného Euklidova algoritmu jehož výstupem je kromě NSD(9,31) také dvojice celočíselných hodnot $a, b \in \mathbb{Z}$, pro které platí

$$1 = \mathrm{NSD}(9, 31) = a \cdot 9 + b \cdot 31 \ .$$

Tudíž nalezená hodnota $a \pmod{31}$ je multiplikativní inverz prvku 9 v $\mathbb{Z}_{31}$. Rozšířený Euklidův algoritmus na vstupu $(9, 31)$ provede následující kroky:

$$\begin{aligned} a_0 &= 31, \\ a_1 &= 9, \\ a_2 &= 4 = 31 - 3 \cdot 9, \\ a_3 &= 1 = 9 - 2 \cdot 4 = 7 \cdot 9 - 2 \cdot 31. \end{aligned}$$

Poslední hodnota a_3 je hledaný $NSD(9, 31)$, o kterém jsme věděli, že musí vyjít roven 1, protože 31 je prvočíslo. Navíc jsme dostali 1 vyjádřené jako součet celočíselných násobků 9 a 31. Můžeme tedy odvodit, že

$$1 = 7 \cdot 9 - 2 \cdot 31 = 7 \cdot 9 - 2 \cdot 31 \pmod{31} = 7 \cdot 9 \pmod{31} \ .$$

Proto $9^{-1} = 7$ v $\mathbb{Z}_{31}$.

Pro 12 dostáváme:

$$\begin{aligned} a_0 &= 31, \\ a_1 &= 12, \\ a_2 &= 7 = 31 - 2 \cdot 12, \\ a_3 &= 5 = 12 - 7 = 3 \cdot 12 - 31, \\ a_4 &= 2 = 7 - 5 = 31 - 2 \cdot 12 - 3 \cdot 12 + 31 = 2 \cdot 31 - 5 \cdot 12, \\ a_5 &= 3 = 5 - 2 = 3 \cdot 12 - 31 - 2 \cdot 31 + 5 \cdot 12 = 8 \cdot 12 - 3 \cdot 31, \\ a_6 &= 1 = 3 - 2 = 8 \cdot 12 - 3 \cdot 31 - 2 \cdot 31 + 5 \cdot 12 = 13 \cdot 12 - 5 \cdot 31. \end{aligned}$$

Opět jsme dostali 1 vyjádřené jako součet celočíselných násobků 12 a 31. Můžeme tedy odvodit, že

$$1 = 13 \cdot 12 - 5 \cdot 31 = 13 \cdot 12 - 5 \cdot 31 \pmod{31} = 13 \cdot 12 \pmod{31} \ .$$

Proto $12^{-1} = 13$ v $\mathbb{Z}_{31}$.

Cv. 8. V $\mathbb{Z}_7$ spočítejte mocninu matice A^{100} pro matici $A = \left(\begin{smallmatrix} 3 & 2 \\ 1 & 4 \end{smallmatrix}\right)$.

Řešení:
Nad konečným tělesem musí být posloupnost matic A^i pro $i = 1, \ldots, \infty$ cyklická. Spočtěme několik prvních členů této posloupnosti:

$$
\begin{aligned}
A = A^1 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} , \\
A^2 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} , \\
A^3 &= \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} , \\
A^4 &= \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} , \\
A^5 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} , \\
A^6 &= \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \\
A^7 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = A .
\end{aligned}
$$

Vidíme, že perioda této posloupnost je 6. Hledanou mocninu matice tedy spočítáme jako

$$A^{100} = A^{100 \pmod 6} = A^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} .$$