

Grupy a tělesa

Grupy

Cv. 5.1 Zjistěte, zda je (Abelovou) grupou:

- (a) $(\mathbb{Q}, +)$,
- (b) $(\mathbb{Q}, -)$,
- (c) $(\mathbb{Q}, \cdot)$,
- (d) $(\mathbb{Q} \setminus \{0\}, \circ)$, kde $a \circ b = |ab|$ pro všechna $a, b \in \mathbb{Q}$,
- (e) $(\mathbb{Q}, \circ)$, kde $a \circ b = \frac{a+b}{2}$ pro všechna $a, b \in \mathbb{Q}$,
- (f) $(\mathbb{Q}, \circ)$, kde $a \circ b = a + b + 3$ pro všechna $a, b \in \mathbb{Q}$,
- (g) $(\mathcal{F}, +)$, tj. množina $\mathcal{F}$ všech reálných funkcí jedné proměnné s operací sčítání funkcí,
- (h) množina rotací v $\mathbb{R}^2$ kolem počátku s operací skládání zobrazení,
- (i) množina posunutí v $\mathbb{R}^2$ s operací skládání zobrazení.

Řešení:

- (a) $(\mathbb{Q}, +)$ je Abelovou grupou:
 - sčítání je komutativní i asociativní operace,
 - neutrální prvek je 0
 - k racionálnímu číslu q je inverzní prvek $-q$.
- (b) $(\mathbb{Q}, -)$ není grupou, protože rozdíl racionálních čísel není asociativní operace. Například $(8 - 6) - 1 = 1 \neq 3 = 8 - (6 - 1)$.
- (c) $(\mathbb{Q}, \cdot)$ není grupou. Součin je sice komutativní i asociativní operace a existuje neutrální prvek 1, ale k číslu 0 neexistuje inverzní prvek.
- (d) $(\mathbb{Q} \setminus \{0\}, \circ)$ s operací $a \circ b = |ab|$ není grupou, protože není zaručena existence neutrálního prvku. Pro každé $a < 0$ a číslo e je $a \circ e = |ae| > 0 > a$. Tudíž žádné e nemůže splňovat definici neutrálního prvku pro záporná a .
- (e) $(\mathbb{Q}, \circ)$ s operací $a \circ b = \frac{a+b}{2}$ není grupou, protože aritmetický průměr čísel není asociativní. Například pro $a = 1$, $b = 5$, $c = 7$ máme $a \circ (b \circ c) = \frac{1}{2} \left(1 + \frac{5+7}{2}\right) = 3.5 \neq 5 = \frac{1}{2} \left(\frac{1+5}{2} + 7\right) = (a \circ b) \circ c$.
- (f) $(\mathbb{Q}, \circ)$ s operací $a \circ b = a + b + 3$ je Abelovou grupou. Asociativita a komutativita platí z asociativity a komutativity 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 k prvku $a \in \mathbb{Q}$ je $a^{-1} = -a - 6$, protože

$$a \circ a^{-1} = a + (-a - 6) + 3 = -3 = e = -3 = (-a - 6) + a + 3 = a^{-1} \circ a.$$

- (g) $(\mathcal{F}, +)$ 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 k funkci $f \in \mathcal{F}$ je funkce $-f$.
- (h) Množina rotací v $\mathbb{R}^2$ kolem počátku je Abelovou grupou. Asociativita plyne z asociativity skládání zobrazení. Komutativita platí také, protože uvažujeme rotace v rovině. Neutrálním prvkem je například rotace o 360 stupňů. Inverzním prvkem k rotaci o úhel α je rotace o úhel α v opačném směru.
- (i) Množina posunutí v $\mathbb{R}^2$ je Abelovou grupou. Asociativita plyne z asociativity skládání zobrazení a komutativita z komutativity sčítání vektorů. Neutrálním prvkem je identické zobrazení $e((x_1, x_2)^T) = (x_1, x_2)^T$ (tj. posunutí vektorem $(0, 0)^T$) a inverzním prvkem k 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. 5.2 Vyplňte tabulku pro binární operaci $\circ$ na G tak aby $(G, \circ)$ byla grupou s neutrálním prvkem 0. Výsledek 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:

Všechny tabulky až na poslední jsou určeny jednoznačně. Fakt, že 0 je neutrálním prvkem pro $\circ$ určuje první řádek i sloupec tabulky. Existence levé i pravé inverze 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 grupa modulo 2, tj. $(\mathbb{Z}_2, +)$

(b)

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

... aditivní grupa modulo 3, tj. $(\mathbb{Z}_3, +)$

(c)

$\circ$	0
0	0

 ... triviální grupa,

(d)

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

, anebo

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

.

První je Kleinova grupa symetrií obdélníka, a to druhé je $(\mathbb{Z}_4, +)$ s přejmenovanými čísly (prohozena 1 a 2).

Cv. 5.3 Rozhodněte a zdůvodněte, zda je Abelovou grupou množina

$$\left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}; z \in \mathbb{Z} \right\} \text{ s maticovým součinem.}$$

Řešení:

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

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}, \quad (1)$$

což je matice náležející do zadané množiny (neboť celá čísla jsou uzavřená na součet).

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 (volbou $z := 0 \in \mathbb{Z}$).

Inverzním prvkem pro matici $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ je celočíselná matice $\begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}$, 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 $\mathbb{Z}$. I když obecně součin matic není komutativní, pro naši třídu matic komutativita splněna jest.

Ověřili jsme tedy, že se jedná o Abelovskou grupu.

Cv. 5.4 Mějme grupu $(G, \circ)$ s neutrálním prvkem e a inverze k prvku a nechť je a^{-1} . Proveďte:

- (a) najděte e^{-1} ,
- (b) upravte $(a \circ b)^{-1}$.

Řešení:

- (a) $e^{-1} = e$, neboť $e \circ e = e$.

(b) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ neboť

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e$$

a analogicky v opačném pořadí.

Cv. 5.5 Najděte různé příklady podgrup grupy matic $(\mathbb{R}^{n \times n}, +)$.

Řešení:

Příkladem je nespočet. Podgrupou je taková (neprázdňá) podmnožina matic $\mathbb{R}^{n \times n}$, která je uzavřená na násobky a součty. Příkladem je tak například podgrupa symetrických matic. Dalšími příklady jsou trojúhelníkové matice, horní trojúhelníkové matice, diagonální matice, matice s racionálními čísly, matice s celými čísly, atp.

Konečná tělesa $\mathbb{Z}_p$

Cv. 5.6 Vyjádřete jako prvky daného tělesa výrazy:

- (a) $((2^{-1} + 1)4)^{-1}$ a $4/3$ v tělese $\mathbb{Z}_5$,
 (b) $6 + 7$, -7 , $6 \cdot 7$, 7^{-1} a $6/7$ v tělese $\mathbb{Z}_{11}$.

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. Pro názornost uvádíme tabulky pro obě operace.

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

$\mathbb{Z}_5, \cdot$	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

Podle definice tělesa má množina $\mathbb{Z}_5 \setminus \{0\} = \{1, 2, 3, 4\}$ se součinem modulo 5 tvořit Abelovu grupu; zde je to takzvaná multiplikativní grupa modulo 5. V tabulce můžeme některé vlastnosti grupy snadno nahlédnout, například komutativitu nebo existenci neutrálního a inverzního prvku.

Nyní můžeme vyhodnotit zadané výrazy v $\mathbb{Z}_5$, kde při výpočtu nalezneme multiplikativní inverzi k libovolnému $a \in \mathbb{Z}_5 \setminus \{0\}$ v tabulce tak, že v řádce s a najdeme hodnotu 1 a index b odpovídajícího sloupce musí být hledaná multiplikativní inverze 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:

$$6 + 7 = 6 + 7 \pmod{11} = 13 \pmod{11} = 2 \text{ v } \mathbb{Z}_{11},$$

$$-7 = 11 - 7 \pmod{11} = 4 \text{ v } \mathbb{Z}_{11}.$$

$$6 \cdot 7 = 6 \cdot 7 \pmod{11} = 42 \pmod{11} = 9 \text{ v } \mathbb{Z}_{11}.$$

Při hledání multiplikativní inverze 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 na pravé straně číslo 1:

$$7 \cdot 1 = 7,$$

$$7 \cdot 2 = 3,$$

$$7 \cdot 3 = 10,$$

$$7 \cdot 4 = 6,$$

$$7 \cdot 5 = 2,$$

$$7 \cdot 6 = 9,$$

$$7 \cdot 7 = 5,$$

$$7 \cdot 8 = 1.$$

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

$$3x + 2y + z = 1,$$

$$4x + y + 3z = 3$$

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. 5.8 Invertujte matici A nad tělesem $\mathbb{R}$, $\mathbb{Z}_3$ a $\mathbb{Z}_5$:

$$A = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 1 & 2 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 2 & 0 & 0 \end{pmatrix}.$$

Řešení:

Gaussovou eliminací dostaneme nad tělesem $\mathbb{R}$ inverzní matici

$$A^{-1} = \begin{pmatrix} 2/3 & 4/3 & -4/3 & -1 \\ -1/3 & -2/3 & 2/3 & 1 \\ 1/3 & -1/3 & 1/3 & 0 \\ -1/3 & 4/3 & -1/3 & -1 \end{pmatrix}.$$

Pro tělesa $\mathbb{Z}_3$ a $\mathbb{Z}_5$ postupujeme podobně, ale s využitím modulární aritmetiky.

V $\mathbb{Z}_3$ dostaneme po přičtení dvojnásobku 1. řádku ke 2. řádku přesně 3. řádek, matice je tedy singulární a inverzní matice neexistuje.

Pro výpočet v $\mathbb{Z}_5$ postupujeme stejně, stačí používat operace přičtení vhodného násobku řádku s pivotem k dalším řádkům a násobení řádku inverzním prvkem k prvku na pozici pivota:

$$\begin{pmatrix} 1 & 1 & 2 & 0 & | & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 1 & | & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & | & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & | & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 0 & | & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 1 & | & 4 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & | & 0 & 0 & 1 & 0 \\ 0 & 1 & 3 & 0 & | & 4 & 0 & 0 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 1 & 2 & 0 & | & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 1 & | & 4 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & | & 1 & 4 & 1 & 0 \\ 0 & 0 & 4 & 4 & | & 0 & 4 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 & 0 & | & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 1 & | & 4 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & | & 2 & 3 & 2 & 0 \\ 0 & 0 & 0 & 4 & | & 2 & 2 & 2 & 1 \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & 1 & 2 & 0 & | & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 1 & | & 4 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & | & 2 & 3 & 2 & 0 \\ 0 & 0 & 0 & 1 & | & 3 & 3 & 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & | & 4 & 3 & 2 & 4 \\ 0 & 1 & 0 & 0 & | & 3 & 1 & 4 & 1 \\ 0 & 0 & 1 & 0 & | & 2 & 3 & 2 & 0 \\ 0 & 0 & 0 & 1 & | & 3 & 3 & 3 & 4 \end{pmatrix}.$$

Nad tělesem $\mathbb{Z}_5$ tedy dostáváme inverzní matici $A^{-1} = \begin{pmatrix} 4 & 3 & 2 & 4 \\ 3 & 1 & 4 & 1 \\ 2 & 3 & 2 & 0 \\ 3 & 3 & 3 & 4 \end{pmatrix}.$

Správnost řešení můžeme také ověřit ze vztahu $AA^{-1} = I_4$.

Cv. 5.9 V $\mathbb{Z}_7$ spočítejte mocninu matice A^{100} pro matici $A = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}$.

Řešení:

Nad konečným tělesem musí být posloupnost matic A^i pro $i = 1, \dots, \infty$ 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 posloupnosti je 6. Hledanou mocninu matice tedy spočítáme jako

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

Poznámka. Trochu práce si můžeme ušetřit tím, že si uvědomíme, že druhá mocnina má tvar $A^2 = 4I_2$. Tudíž

$$A^{100} = (A^2)^{50} = (4I_2)^{50} = 4^{50}I_n.$$

Tím jsme maticový problém zredukovali na skalární problém. Z Malé Fermatovy věty víme, že $4^6 = 1$ v $\mathbb{Z}_7$, čili

$$4^{50}I_n = 4^{50 \pmod{6}}I_n = 4^2I_n = 2I_n.$$

Cv. 5.10 Spočítejte 20^{3332} v tělese $\mathbb{Z}_{31}$.

Řešení:

Z Malé Fermatovy věty víme, že v tělese $\mathbb{Z}_{31}$ je $20^{30} = 1$. Proto

$$20^{3332} = 20^{3332 \pmod{30}} = 20^2 = 28.$$