cvičení Lineární algebra

II Grupy a tělesa

- $(G, \circ)$ $\circ$ je asociativní $\forall g,h,k \in G$ $g\circ(h\circ k)=(g\circ h)\circ k$

  $\exists$ jednotkový prvek e $\forall g \in G: g\circ e = e\circ g = g$

  $\forall g \exists g^{-1}$ $g\circ g^{-1} = e = g^{-1}\circ g$

Rozhodněte zda následující jsou grupy:

1) a) $(\mathbb{R},+)$ ✓ b) $(\mathbb{Q}^+,\cdot)$ ✓

c) $(\mathbb{Q}\setminus\{0\},\circ)$ $a\circ b = |ab|$ d) $(\mathbb{Q},\circ)$ $a\circ b := a+b+3$

e) Otočení kolem počátku v rovině, $\circ$ skládání zobrazení.

c) asociativita $(a\circ b)\circ c = ||ab|\cdot c| = |abc|$ ✓

$(a\circ(b\circ c)) = |a\cdot|bc|| = |abc|$

neutrální prvek $\exists e$ $\forall q \in \mathbb{Q}\setminus\{0\}$ $e\circ q = q$ q je záporné $\Rightarrow x\circ q$ kladné $\forall x \in \mathbb{Q}\setminus\{0\}$

$\rightarrow$ nemá jednotkový prvek ✗

d) asociativita: $(a\circ b)\circ c = a+b+c+6$ ✓ $(a\circ b)\circ c = (a+b+3)\circ c = (a+b+3)+c+3 = a+b+c+6$

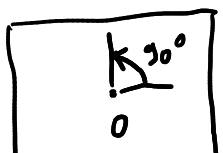
$(a\circ(b\circ c)) = a+b+c+6$

$e = -3$

$\forall q$ $\exists q^{-1}$ $q\circ q^{-1} = -3 = q^{-1}\circ q$

$q + q^{-1} + 3 = -3$

$q^{-1} = -q-6$

e) 

✓

- skládání zobrazení je asociativní
- neutrální prvek otočení o $0°, 360°, \ldots$
- opačný prvek k otočení o α po směru hodinových ručiček, otočení o α proti směru

f) $(\mathbb{Q},\circ)$ $a\circ b = \frac{a+b}{2}$ ✗

není asociativní

a,b,c

Doplňte tak, aby šlo o grupus neutrálním prvkem 0.

a)

∘	0	1
0		
1		

b)

∘	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

c)

∘	0
0	0

d)

∘	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

👁 Kvůli existenci inverzního prvku, je v každém řádku i sloupci každé číslo právě jednou

(akorát musíme ověřit asociativitu...)

$a \circ (e \circ b) = a \circ b$ $\quad ((e \circ a) \circ b) = a \circ b$

$(a \circ e) \circ b = a \circ b$ $\quad e \circ (a \circ b) = a \circ b$

Těleso $(T, +, \cdot)$

- $(T, +)$ je grupa s neutrálním prvkem 0
- $(T \setminus \{0\}, \cdot)$ je grupa
- distributivní zákony

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a,b,c \in T$$

$$(a+b) \cdot c = a \cdot c + b \cdot c \quad \forall a,b,c \in T$$

Příklady:

a) $(\mathbb{Q}, +, \cdot)$ ✓

b) $(\mathbb{C}, +, \cdot)$ ✓

c) Matice 2×2 s reálnými čísly a maticovým +, · ✗ $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ nemá inverz

d) $(\mathbb{Z}, +, \cdot)$ ✗ $2^{-1} \notin \mathbb{Z}$

e) čísla $0, 1, 2, \dots, n-1$ s + modulo n, · modulo n

Zjistěte o n: n prvočíslo, tak ano, jinak ne

$n = 5$

+	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

·	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

$3^{-1} = 2$

$\mathbb{Z}_5$ nebo $\mathbb{Z}/5\mathbb{Z}$ nebo $GF(5)$

- Od teď matice a rovnice nad libovolným tělesem.
- Nad $\mathbb{Z}_5$ vyřešte

$$\left(\begin{array}{cc|c} 1 & 3 & 0 \\ 2 & 4 & 1 \end{array}\right) \overset{2+3x}{\sim} \left(\begin{array}{cc|c} 1 & 3 & 0 \\ 0 & 3 & 1 \end{array}\right) \cdot 2$$

$$\sim \left(\begin{array}{cc|c} 1 & 3 & 0 \\ 0 & 1 & 2 \end{array}\right) \overset{5}{\underset{2x}{\sim}} \left(\begin{array}{cc|c} 1 & 0 & 4 \\ 0 & 1 & 2 \end{array}\right)$$

Jak najít inverzní prvek? $GF(5)$, $GF(100003)$

$2^{-1} = ?$ Řešení: Rozšířený Euklidův algoritmus na výpočet $nsd(a,b)$.

a, b čísla

a	1	0
b	0	1
1	r	s

druhý sloupec $\times a$
třetí sloupec $\times b$
= první sloupec

předposlední řádku odečtu $\lfloor \frac{a}{b} \rfloor \times$ od předposlední

$ra + sb = 1$

• určete r, s tak, že $r \cdot 97 + s \cdot 36 = 1$

97	1	0	5	$97/36 = 2$ zbytek 25
36	0	1	$-2\times$	
25	1	-2	$-1\times$	$36/25 = 1$ zbytek 11
11	-1	3	$-2\times$	$25/11 = 2$ zbytek 3
3	3	-8	$-3\times$	$11/3 = 3$ zbytek 2
2	-10	27	$-1\times$	$3/2 = 1$ zbytek 1
1	13	-35	$-2\times$	$2/1 = 2$ zbytek 0
0	-36	97		

$\Rightarrow 1 = \boxed{13 \cdot 97} + (-35) \cdot 36$

Neboli v $\mathbb{Z}_{97}$: $-35 = 36^{-1}$ $\quad (-35) \cdot 36 \equiv 1 \mod 97$

---

1) Nad $\mathbb{Z}_5$ vyřešte: $3x + 2y + z = 1$, $4x + y + 3z = 3$. Kolik řešení existuje?

2) Spočtěte 9^{-1} a 12^{-1} v $\mathbb{Z}_{31}$. (Rozšířený Euklidův algoritmus)

3) Spočtěte A^{100} pro $A = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}$ nad $\mathbb{Z}_7$.

$\left\{ \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix} + t \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix} + s \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} ; t, s \in \mathbb{Z}_5 \right\}$