OPAKOVÁNÍ

LA1 | 6/11/2023

Grupy: Dvojice $(G, \square)$, kde G je množina a $\square$ je binární operace splňující:

Příklad - permutace

1. $\forall a,b,c \in G : (a \square b) \square c = a \square (b \square c)$ asoc.
2. $\exists e \in G \; \forall a \in G : a \square e = e \square a = a$ neutr.
3. $\forall a \in G \; \exists b \in G : a \square b = b \square a = e$ inverz.

Abelova grupa: navíc 4. $\forall a,b \in G : a \square b = b \square a$ kom.

Definice: **Těleso** je množina T spolu se dvěma binárními operacemi $+$ (sčítání) a $\cdot$ (násobení), splňujícími následující podmínky (tzv. axiomy):

1) $(T, +)$ je Abelova grupa s neutrálním prvkem 0, inverzní prvek k a značíme $-a$
2) $(T \setminus \{0\}, \cdot)$ je Abelova grupa s neutrálním prvkem 1, inverzní prvek k a značíme a^{-1}
3) $\forall a,b,c \in T : a \cdot (b+c) = a \cdot b + a \cdot c$ (distributivita)

Poznámky:

- T má vždy aspoň 2 prvky ... $0, 1$
- operaci $+$ říkáme **sčítání**, $\cdot$ **násobení**
- dvě odvozené binární operace:
  $\forall a,b \in T : a - b = a + (-b)$ **odčítání**
  $\forall a \in T, b \in T \setminus \{0\} : a / b = a \cdot b^{-1}$ **dělení**

Příklady: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ s obvyklým $+, \cdot$

Netěleso: $\mathbb{N}, \mathbb{Z}$

$T = \{0, 1\}$.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

← nejmenší těleso (ověřte si) axiomy

Tvrzení 1: 1. Prvky $0, 1$ jsou určeny jednoznačně.

2. $\forall a \in T$, prvek $-a$ určen jednoznačně

3. $\forall a \in T \setminus \{0\}$, prvek a^{-1} určen jednoznačně.

Důkaz: platí už pro grupy.

1. Předp. $0, \bar{0}$: $0 = 0 + \bar{0} = \bar{0}$.

2. $-a = -a + 0 = -a + (a + (\overline{-a}) = (-a + a) + (\overline{-a}) = \overline{-a}$

pro $\cdot, a^{-1}$ stejně ∎

Tvrzení 2: 1. $\forall a \in T$, $0 \cdot a = 0 = a \cdot 0$ (nemusíme psát, že $a \cdot 0 = 0a$)

2. $\forall a \in T$, $(-1) \cdot a = -a$

3. Platí $a \cdot b = 0$, pak $a = 0$ nebo $b = 0$.

Důkaz: 1. $0 \cdot a = 0 \cdot a + (0 \cdot a - 0 \cdot a) = (0 \cdot a + 0 \cdot a) - 0a =$

$= (0 + 0) \cdot a - 0 \cdot a = 0 \cdot a - 0 \cdot a = 0$

obdobně $a \cdot 0 = 0$

2. $(-1) \cdot a + a = (-1 + 1) \cdot a = 0 \cdot a = 0$, tj. $(-1)a$ má vlastnost inverzního prvku k a; díky jednoznačnosti (viz Tvrzení 1) musí být $(-1) \cdot a = -a$.

3. sporem: předp. $a \neq 0, b \neq 0$. Protože $(T \setminus \{0\}, \cdot)$ je grupa, je $T \setminus \{0\}$ uzavřená na násobení, tedy $a \cdot b \neq 0$ → spor ∎

Př. $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ (DM: zbytkové třídy)

sčítáme a násobíme se provádí tzv. "modulo n"

značení: pro celé číslo $c \in \mathbb{Z}$, $c \bmod n$ označuje $d \in \mathbb{Z}_n$ tj. n dělí $c - d$

Zavedeme operace $\oplus, \odot$:

$a \oplus b = (a + b \bmod n)$

$a \odot b = (a \cdot b \bmod n)$

"hodinová" aritmetika:

10 hodin + 3 hodiny = 1 hodina

Kdy je $(\mathbb{Z}_n, \oplus, \odot)$ těleso?

Věta: $\mathbb{Z}_n$ je těleso $\iff$ n je prvočíslo.

Důkaz: $\Rightarrow$ sporem. Předp. $\mathbb{Z}_n$ je těleso & $n = a \cdot b$, $a, b > 1$

pak $a \odot b = 0$ – spor s Tvrzení 2, bod 3.

$\Leftarrow$ je třeba ověřit všechny axiomy

většina snadná

? $\forall a \in \mathbb{Z}_n \setminus \{0\} \; \exists a^{-1}$ tž. $a \cdot a^{-1} = 1$

☺ čísla $1 \odot a, 2 \odot a, \dots, (n-1) \odot a$ jsou navzájem různá.

dk. když $c \odot a = d \odot a$ pro $c \neq d$, tak

$$0 = d \odot a - c \odot a = (d - c) \odot a$$

dle předchozího Tvrzení buď $d - c = 0$, tj. $d = c$,

— nebo $a = 0$ – ani jedno nepřipadá.

$\Rightarrow$ mezi $n-1$ různými nenulovými (!) čísly z $\mathbb{Z}_n$

– jedno z nich musí být 1, tedy pro

nějaké $b \in \{1, \dots, n-1\}$ máme $a \odot b = 1$ ∎

Pozn. Existenční důkaz – víme, že $\exists$, nevíme, které.

Věta (malá Fermatova)

Buď n prvočíslo a buď $a \neq 0$, $a \in \mathbb{Z}_p$. Pak

$$\underbrace{a \odot a \odot \cdots \odot a}_{\text{součin } n-1 \text{ čísel } a} = 1 \qquad (a^{n-1} = 1 \mod n)$$

Důkaz: v minulém důkazu jsme si všimli:

$$\{1, 2, \dots, n-1\} = \{1 \odot a, 2 \odot a, \dots, (n-1) \odot a\}$$

$\Rightarrow$ součin čísel v obou množinách je stejný:

$$1 \odot 2 \odot \cdots \odot (n-1) = 1 \odot a \odot 2 \odot a \odot \cdots \odot (n-1) \odot a$$

asociativita, inverzní pr. $\Rightarrow$ $1 = \underbrace{a \odot a \odot \cdots \odot a}_{(n-1) \text{ krát}}$ ∎

Důsledek: inverzní prvek k a je a^{n-2}.

PERMUTACE

Def. **Permutace** množiny X je vzájemně jednoznačné zobrazení (tzv. bijekce) $\pi : X \to X$.

S_n ... množina všech permutací $\{1, 2, \dots, n\}$

Reprezentace: • **dvouřádkový zápis**: $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$

• **šipkami**:

Skládání permutací: jako u zobrazení. Pro $\rho, \sigma \in S_n$,

$\rho \circ \sigma$ je definováno předpisem

$$\rho \circ \sigma(i) = \rho(\sigma(i))$$

$(S_n, \circ)$ je grupa. asociativ., identita, inverze

Dvojice (i, j) je **inverze** permutace $\pi \in S_n$,

pokud $i < j$ & $\pi(i) > \pi(j)$

tj. křížení šipek

$I(\pi)$ ... množina všech inverzí π

Znaménko permutace: $\operatorname{sgn}(\pi) = (-1)^{|I(\pi)|}$ ↗ sudé ... +1, ↘ liché ... −1

Transpozice: permutace, která mění jen dva prvky

Def: Pokud existuje n t.ž. $\underbrace{1+1+\cdots+1}_{n\text{-krát}} = 0$, pak nejmenší takové n nazýváme **charakteristika** tělesa;
v opačném případě je charakteristika nula.

Věta: Charakteristika tělesa je buď 0 nebo prvočíslo.

Důkaz: předp. charakteristika je $n = a \cdot b$, $a, b > 1$

pak $0 = \underbrace{\underbrace{1+1+\cdots+1}_{a\text{-krát}} + \underbrace{1+1+\cdots+1}_{a\text{-krát}} + \cdots + \underbrace{1+1+\cdots+1}_{a\text{-krát}}}_{b\text{-krát}}$ (n-krát)

$= \underbrace{(1+1+\cdots+1)}_{a\text{-krát}}\underbrace{(1+1+\cdots+1)}_{b\text{-krát}} = a \cdot b$ ↑ - spor

součin nenulových není nula ☒

distributivita použita opakovaně

Příklad tělesa na 4 prvcích:

$T = \{0, 1, x, (x+1)\}$

sčítání: jako sčítání polynomů, dle koeficientů počítáme mod 2

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

násobení: jako násobení polynomů mod x^2+x+1

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x^2 \bmod (x^2+x+1) = -(x+1) = x+1$

$x^2+1 \bmod (x^2+x+1) = 1$

$(x+1)^2 \bmod (x^2+x+1) = x$

(Platí: Těleso s n prvky existuje $\Leftrightarrow$ n je mocnina prvočísla.) 6-5