# VLASTNOSTI OPERACÍ
## (ALGEBRAICKÉ STRUKTURY)

Vlastnosti operace (binární) $*$ na množině $A$

komutativita (= nezáleží na pořadí)

$\forall a \forall b$ platí $a * b = b * a$

asociativita (= překážvorchorání)

$\forall a \forall b \forall c$ platí $a * (b * c) = (a * b) * c$

neutrální prvek $\exists e \forall a \quad e * a = a * e$

mít všechny inverzi $\forall a \exists a^{-1} \quad a * a^{-1} = e = a^{-1} * a = e$

→ $e$ = nulární operace

$(-)^{-1}$ = unární operace

distributivita - pro 2 binární operace na $A$ $\oplus$ $\odot$

→ $\odot$ vůči $\oplus$

$\forall a \forall b \forall c \quad a \odot (b \oplus c) = (a \odot b) + (a \odot c)$

### Množina s 1 binární operací

GRUPOID = $(A, *)$ $*: A \times A \to A$ binár. operace (def. všude, výsl. z $A$)

POLYGRUPA = grupoid, kde $*$ je asociativní

MONOID = —"— a má neutrál

GRUPA = —"— má všechny inverzy

komutativita platí všude

## Množina s 2 binár. operacemi

označíme je $+, \cdot$ $\quad (A, +, \cdot)$

OKRUH – $(A, +)$ kom. grupa
$(A, \cdot)$ pologrupa
– distribuk. „$\cdot$" vůči „$+$"

KOM. OKRUH s 1
– okruh, kde „$\cdot$" je komut. a má neutrál

TĚLESO (kom) – kom. okruh s 1, kde všechny nenulové prvky mají ~~inv~~ inverz
– $(A, +)$
$(A \setminus \{0\}, \cdot)$ } kom. grupy
+ distrib

(PŘ1) Určete vlastnosti operací

$(A = \langle 0, 1 \rangle, *)$
$x * y = x \cdot y^2$
Je to grupoid? $\quad * : A \times A \to A$

pro $0 \le x, y \le 1 \to 0 \le y^2 \le 1$
$0 \le x \cdot y^2 \le 2$

Ano, $*$ je binár. operace na $A$.

Pozn: $(B = \langle 0, 2 \rangle, *)$ není ani grupoid!
$x = y = 1{,}5 \qquad 1{,}5 \cdot 1{,}5^2 > 2$

komut. NE $\quad x * y = x y^2$
$y * x = y x^2$ } $\neq$

asociat. NE

$$x*(y*z) = x*(xyz^2) = x(yz^2) = xy^2z^4$$
$$(x*y)*z = xy^2 \cdot z^2$$
$$\Big\} \neq$$

neutrál

$x*1 = x \cdot 1^2 = x$ → 1 je neutrál zprava

$1*y = 1 \cdot y = y^2$ → neexistuje levý neutrál

zleva e $e*y = ey^2 = y$

$$\Downarrow$$
$$e = \frac{1}{y}$$

e není společné pro všechny $y \in A$

→ není oboustranný neutrál

→ nehledáme inverzi

PŘ2 $A = \{a, b, e\}$ - určit vlastnosti z tabulky

| * | a | b | e |
|---|---|---|---|
| a | a | b | e |
| b | b | e | a |
| e | e | a | b |

$b * a = b$

komut. ANO - tabulka je symetrická dle diagonály

neutrál a - přiřazuje každému sloupec (= pravý neutrál) řádek (= levý neutrál)

inverzy $a^{-1} = a$ v každém ř. i sl. je neutrál

$b^{-1} = c$

$c^{-1} = b$

asociat. - nejde poznat z tabulky

když $(A, *)$ je $(\mathbb{Z}_3, +) \Rightarrow$ je asociat.

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

$\Rightarrow$ komut. grupa

PŘ 3

$\mathcal{F} = \{f : \{0,1\} \to \{0,1\}\}$

$*$ - obrácení skládání fcí

$f * g$ - fce l. č. $(f * g)(x) = g(f(x)) = (g \circ f)(x)$

Prvky v $\mathcal{F}$

id: $0 \to 0$, $1 \to 1$

$f_0$: $0 \to 0$, $1 \to 1$

$g$: $0 \to 0$, $1 \to 1$

$f_1$: $0 \to 0$, $1 \to 1$

každá fce je určena def. oborem a svými vyjádřeními.

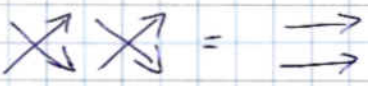
Operace $*$

$f_0 * g$ = $f_1$

| $*$ | id | $f_0$ | $f_1$ | $g$ |
|---|---|---|---|---|
| id | id | $f_0$ | $f_1$ | $g$ |
| $f_0$ | $f_0$ | $f_0$ | $f_1$ | $f_1$ |
| $f_1$ | $f_1$ | $f_0$ | $f_1$ | $f_0$ |
| $g$ | $g$ | $f_0$ | $f_1$ | id |

~~neutrál = id~~

$g * g = id$



$f_0 * f_1 = f_1$

neutrál = id

komutat. NE

inverzy $id^{-1} = id$

$f_0^{-1}, f_1^{-1}$ = nelze id.

$g^{-1} = g$

asociat. ANO ← skládání zobrazení (fcí) JE VŽDY asociativní

$f * (g * h) = \ldots = h(g(f(x)))$

$(f * g) * h = \ldots = h(g(f(x)))$

→ Monoid (nekomut.)

PŘ 4

$B = \{ F = \{ f : \{0,1\} \to \{0,1\} : f \text{ je bijekce} \}$

vzájemně jednoznačná
(kon. je prostá a je na)

$*$ - obrácené skládání

| $*$ | id | $g$ |
|---|---|---|
| id | id | $g$ |
| $g$ | $g$ | id |

$B = \{id, g\}$

$f_0, f_1$ nejsou prosté

→ Grupa

Obecně: Symetrická grupa = grupa permutací na množ. $\{1, 2, \dots, n\}$

$S_n = \{ f : \{1, \dots, n\} \to \{1, \dots, n\},$
$f$ je bijekce $\}$

mohu $f \leftrightarrow (f(1), \dots, f(n))$ n-tice vzájemných

pro $f$ bijekci je $(f(1), \dots, f(n))$ permutace množ. $\{1, \dots, n\}$ →

$|S_n| = n!$

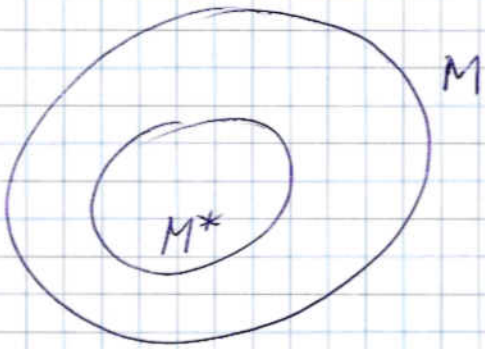
→ množ. má $n!$ prvků

$(S_n, *)$

↑ obrácené skládání je nekomut. grupa
($e = id$, $f^{-1}$ bijekce má inverz. zobr.)

**Tvrzení:** Je-li množ. $(M, \circ)$ monoid, pak
$M^* = \{a \in M, \text{ exist. } a^{-1} \in M\}$
$(M^*, \circ)$ je grupa, tzv. **grupa invertibilních prvků z monoidu**

DK




1) $M^*$ je podmnož. uzavřená na oper. $\circ$
Když $a, b \in M^* \xrightarrow{?} a \circ b \in M^*$

↓

exist. $a^{-1}, b^{-1}$ → ukážu, že $(b^{-1} \circ a^{-1})$ je inverze k $(a \circ b)$

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

asociat. (M monoid) — e neutrál (M monoid)

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

2) $\circ$ je asociat. na $M^*$
ANO, neboť zůstávorkovat lze na celé $M$

3) $e \in M^*$, neboť lze $e^{-1} = e$

$(M^*, \circ)$ je grupa

4) $M^*$ je uzavřená na inverzy
$a \in M^* \rightarrow a^{-1} \in M^*$, neboť lze $(a^{-1})^{-1} = a$

PŘ $(\mathbb{Z}_n, \cdot)$ kom. monoid

(ne grupa $\leftarrow$ $0^{-1}$ není)

$(\mathbb{Z}_n^*, \cdot)$ kom. grupa

pime, že $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n,\ a \text{ nesoud. } n\}$

$|\mathbb{Z}_n^*| = \varphi(n)$

např. $\mathbb{Z}_6^* = \{1, 5\}$

| $\cdot$ | 1 | 5 |
|---|---|---|
| 1 | 1 | 5 |
| 5 | 5 | 1 |

$5 \cdot 5 = 25 = 1 \in \mathbb{Z}_6$

ALE $(\mathbb{Z}_6^*, +)$ není ani grupoid

| $+$ | 1 | 5 |
|---|---|---|
| 1 | 2 | |
| 5 | | |

$1 + 1 = 2 \notin \mathbb{Z}_6^*$ !