Vlastnosti binárních operací:

Definice : Binární operace $\circ$ v množině M, která má vlastnost, že je definována pro každou uspořádanou dvojici $[x,y] \in$ M x M, se nazývá operace **neomezeně definovaná** v množině M (zkráceně operace **definovaná na** množině M). Značíme **ND**.

Symbolicky: $x, y \in \mathrm{M})(\exists\, z \in \mathrm{M})[\, x \circ y = z]$.

Definice: Binární operace $\circ$ definovaná na množině M (je ND), se nazývá **komutativní** právě tehdy, když platí:

$$x, y \in \mathrm{M})[\, x \circ y = y \circ x].$$

Značíme **K**.

Definice: Binární operace $\circ$ definovaná na množině M, se nazývá **asociativní** právě tehdy, když platí:

$$x, y, z \in \mathrm{M})[\, (x \circ y) \circ z = x \circ (y \circ z)].$$

Značíme **A**.

Definice: Nechť v množině M je definována binární operace $\circ$. Existuje-li prvek $e \in$ M, pro který platí:

$$x \in \mathrm{M})[\, x \circ e = e \circ x = x].$$

Pak se prvek $e \in$ M nazývá **neutrálním prvkem** množiny M vzhledem k operaci $\circ$.
Značíme **EN**.

Poznámka. Je-li operace $\circ$ komutativní, pak v zápisu vlastnosti **EN** lze vynechat jedna ze dvou stran rovnosti $x \circ e$ nebo $e \circ x$.

Definice : Nechť v množině M je definována binární operace $\circ$ a nechť e je neutrální prvek množiny M vzhledem k operaci $\circ$. Prvek $\bar{a} \in$ M nazýváme **inverzním prvkem** k prvku $a \in$ M v operaci $\circ$ v množině M právě tehdy, když platí:

$$\bar{a} \circ a = a \circ \bar{a} = e.$$

Jestliže $(a \in \mathrm{M})(\exists\, \bar{a} \in \mathrm{M})[\, \bar{a} \circ a = a \circ \bar{a} = e]$, řekneme, že ke každému prvku množiny M existuje prvek inverzní vzhledem k operaci $\circ$. Značíme **EI**.

Poznámka . Je-li operace $\circ$ komutativní, pak v zápisu vlastnosti **EI** lze vynechat jedna ze dvou stran rovnosti $\bar{a} \circ a = a \circ \bar{a}$.

Definice : Říkáme, že binární operace $\circ$ definovaná na množině M má vlastnost **řešitelnost základních rovnic** právě tehdy, když platí:

$$a, b \in \mathrm{M})\ )(\exists\ x, y \in \mathrm{M})[\ a \circ x = b \quad y \circ a\ = b].$$

Značíme **ZR**.

Poznámka. Je-li operace $\circ$ komutativní, pak v zápisu vlastnosti **ZR** lze vynechat jedna z výrokových forem $a \circ x = b$ nebo $y \circ a\ = b$.

Definice: Nechť v množině M je definována binární operace $\circ$. Existuje-li prvek $g \in \mathrm{M}$, pro který platí:

$$x \in \mathrm{M})[\ x \circ g = g \circ x = g].$$

Pak se prvek g nazývá **agresivním** prvkem množiny M vzhledem k operaci $\circ$.

Určování vlastností operací

I. **Určených předpisem** – přímým výpočtem

II. **Určených tabulkou**:

ND – tabulka zcela vyplněna prvky množiny M

K – tabulka souměrná podle hlavní diagonály

A – kromě výjimek nelze z tabulky přímo poznat – viz dále

EN – existuje řádek a sloupec shodný se záhlavím tabulky

EI – v každém řádku a každém sloupci tabulky je neutrální prvek

ZR – v každém řádku i sloupci tabulky jsou všechny prvky množiny M

Agresivní prvek $g \in \mathrm{M}$ poznáme tak, že v celém jemu příslušejícím řádku i sloupci se vyskytuje pouze prvek g.

Užitečné vztahy: K $\Rightarrow$ ND, A $\Rightarrow$ ND, EI $\Rightarrow$ EN (užívají se v obměněném tvaru)

$$\mathrm{A} \Rightarrow (\mathrm{EI} \Leftrightarrow \mathrm{ZR})$$

Určování asociativnosti z tabulek:

1. Pohledem (velmi zřídka)

2. Ověřením všech možných trojic prvků (s využitím cvičení 9 – 13 v učebnici, s. 123 – 124) (těžkopádné a zdlouhavé)

3. Využitím obměny implikace A $\Rightarrow$ ND a implikace A $\Rightarrow$ (EI $\Leftrightarrow$ ZR)

4. Podle tvrzení: „ Operace, která splňuje EN $\wedge$ EI $\wedge$ ZR a současně není asociativní, existuje na množině o nejméně pěti prvcích“.

Užití na příkladech:

ad 1. Např.

o	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

ad 3. Nejčastější případ – rozbor implikace A $\Rightarrow$ (EI $\Leftrightarrow$ ZR). Je-li u EI a ZR rozdílná pravdivostní hodnota, pak operace není asociativní. Jsou-li u EI a ZR pravdivostní hodnoty 1, pak postupujeme podle bodu 4 (v písemných pracích jsou zadávány tabulky o maximálně čtyřech prvcích). Jsou-li u EI a ZR pravdivostní hodnoty 0, pak je nutno postupovat podle bodu 1 nebo 2. Zpravidla jde o bod 1, kdy určíme asociativnost přímo z tabulky.

o	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Má všechny vlastnosti.

Př: Rozhodněte a zdůvodněte, které z vlastností ND, A, K, EN, EI, ZR má v množině M = $\{a,b,c\}$ operace určená tabulkou:

*	a	b	c
a		a	b
b	a	b	c
c	b	c	b

○	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

□	a	b	c
a	c	a	a
b		c	b
c	a	b	c

■	a	b	c
a	a	b	c
b	b	a	c
c	c	b	a

*: ~~ND~~ ∧ ~~K~~ ∧ ~~A~~ ∧ EN ∧ EI ∧ ~~ZR~~

○: ND ∧ ~~K~~ ∧ ~~A~~ ∧ ~~EN~~ ∧ ~~EI~~ ∧ ZR

□: ~~ND~~ ∧ ~~K~~ ∧ ~~A~~ ∧ EN ∧ EI ∧ ~~ZR~~

■: ND ∧ ~~K~~ ∧ ~~A~~ ∧ EN ∧ EI ∧ ~~ZR~~

Př: V množině M = $\{a,b,c\}$ definujte tabulkou aspoň jednu binární operaci, která má vlastnosti:

a) K ∧ ~~EN~~ b) ND ∧ ~~K~~ ∧ EN c) ND ∧ EN ∧ ~~EI~~ d) A ∧ ~~ZR~~

e) ~~K~~ ∧ EN ∧ ~~EI~~ f) EI ∧ ZR g) ND ∧ ~~A~~ ∧ EI ∧ ~~ZR~~ h) ~~A~~ ∧ EN ∧ EI ∧ ZR

a)	a	b	c
a	c	c	b
b	a	b	c
c	b	c	b

b)	a	b	c
a	b	a	a
b	c	b	b
c	a	b	c

c)	a	b	c
a	b	a	a
b	a	c	b
c	a	b	c

d)	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

e)	a	b	c
a		a	b
b	a	b	c
c	c	a	a

f)	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

g)	a	b	c
a	c	a	a
b	a	c	b
c	a	b	c

Nemá			
řešení			

Algebraické struktury s jednou operací

Definice 9: Uspořádaná dvojice (M, ○), kde M je neprázdná množina, ve které je definována binární operace ○, se nazývá **algebraická struktura s jednou operací.**

Příklad 9: Příklad algebraických struktur: ($\mathbb{N}$, +), ($\mathbb{C}$, -), ($\mathbb{Q}$ - {0}, :), ($\mathbb{R}$, ·); (M, ○), kde množina M = {a, b, c} a operace ○ je určena tabulkou.

Definice 10:

I. Algebraická struktura (M, ○) se nazývá **grupoid** právě tehdy, když operace ○ je neomezeně definovaná v množině M (ND).

II. Grupoid (M, ○), jehož operace ○ je asociativní, se nazývá **podgrupa** (ND, A).

III. Pologrupa (M, ○) taková, že v M existuje neutrální prvek vzhledem k operaci (M, ○) a ke každému prvku $a \in$ M existuje prvek inverzní $\bar{a} \in$ M, se nazývá **grupa** (ND, A, EN, EI).

Poznámka 6. Jestliže v případech I., II., III. je operace ○ komutativní, pak hovoříme o

I. Komutativním grupoidu
II. Komutativní pologrupě
III. Komutativní grupě

<u>Schéma k *Definici 10*:</u>

	Vlastnost operace ○	**Algebraická struktura**
(M, ○)	ND	Grupoid
	ND ∧ K	Komutativní grupoid
	ND ∧ A	Pologrupa
	ND ∧ A ∧ K	Komutativní pologrupa
	ND ∧ A ∧ EN ∧ EI	Grupa
	ND ∧ A ∧ EN ∧ EI ∧ K	Komutativní grupa

Poznámka: Operace v grupě má vždy také vlastnost ZR. Plyne z implikace A $\Rightarrow$ (EI $\Leftrightarrow$ ZR). Proto se někdy grupa definuje jako struktura, jejíž operace je ND $\wedge$ A $\wedge$ ZR.

Příklady algebraických struktur s jednou operací

1. ($\mathbb{N}$, +) … komutativní pologrupa
   sčítání … ND $\wedge$ K $\wedge$ A $\wedge$ ~~EN~~ $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~
   rovnice $a + x = b$ není pro libovolné $a, b \in \mathbb{N}$ řešitelná

2. ($\mathbb{N}_0$, +) … komutativní pologrupa s neutrálním prvkem $e = 0$
   sčítání … ND $\wedge$ K $\wedge$ A $\wedge$ EN $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~

3. ($\mathbb{N}_0$, -) … není ani grupoid
   odčítání …~~ND~~ $\wedge$ ~~K~~ $\wedge$ ~~A~~ $\wedge$ ~~EN~~ $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~
   hledáme neutrální prvek, pro který platí: $a - e = e - a = a$
   $a - e = a \;\wedge\; e - a = a$
   $e = 0 \wedge e = 2a$ (vlastnost EN není splněna)

4. ($\mathbb{N}_0$, ·) … komutativní pologrupa s neutrálním prvkem $e = 1$
   násobení …ND $\wedge$ K $\wedge$ A $\wedge$ EN $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~

5. ($\mathbb{N}_0$, :) …není ani grupoid
   dělení… ~~ND~~ $\wedge$ ~~K~~ $\wedge$ ~~A~~ $\wedge$ ~~EN~~ $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~

---

6. ($\mathbb{C}$, +) … komutativní grupa s neutrálním prvkem $e = 0$
   sčítání…ND $\wedge$ K $\wedge$ A $\wedge$ EN $\wedge$ EI $\wedge$ ZR
   $\bar{a} = -a$
   rovnice $a + x = b$ je pro libovolné $a, b \in \mathbb{C}$ řešitelná

7. ($\mathbb{C}$, -) … grupoid s vlasností ZR
   odčítání …ND $\wedge$ ~~K~~ $\wedge$ ~~A~~ $\wedge$ ~~EN~~ $\wedge$ ~~EI~~ $\wedge$ ZR
   operace odčítání není K*:* $a - x = b \wedge y - a = b$
   obě rovnice jsou pro lib. $a, b \in \mathbb{C}$ řešitelné

8. ($\mathbb{C}$, ·) … komutativní pologrupa s neutrálním prvkem $e = 1$
   násobení …ND $\wedge$ K $\wedge$ A $\wedge$ EN $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~
   rovnice $a \cdot x = b$ není pro libovolné $a, b \in \mathbb{C}$ řešitelná

9. ($\mathbb{C}$, :) …není ani grupoid
   dělení… ~~ND~~ $\wedge$ ~~K~~ $\wedge$ ~~A~~ $\wedge$ ~~EN~~ $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~

---

10. ($\mathbb{Q}$, +), ($\mathbb{R}$, +) … komutativní grupy s neutrálním prvkem $e = 0$
sčítání…ND $\wedge$ K $\wedge$ A $\wedge$ EN $\wedge$ EI $\wedge$ ZR

$$\bar{a} = -a$$

rovnice $a + x = b$ je pro libovolné $a, b \in \mathbb{Q}, \mathbb{R}$ řešitelná

11. ($\mathbb{Q}$, -), ($\mathbb{R}$, -)… grupoid s vlastností ZR
odčítání …ND $\wedge$ ~~K~~ $\wedge$ ~~A~~ $\wedge$ ~~EN~~ $\wedge$ ~~EI~~ $\wedge$ ZR

12. ($\mathbb{Q}$, ·), ($\mathbb{R}$, ·)… komutativní pologrupy s neutrálním prvkem $e = 1$
násobení …ND $\wedge$ K $\wedge$ A $\wedge$ EN $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~

~~EI~~: $\bar{a} \cdot a = 1$

$$\bar{a} = \frac{1}{a}$$

pro $a = 0$ však neexistuje $\bar{a}$, neboť výraz $\frac{1}{0}$ není definován

~~ZR~~: $a \cdot x = b$

$$x = \frac{b}{a}$$

pro $a = 0 \wedge b \neq 0$ však neexistuje $x \in \mathbb{Q}, \mathbb{R}$ tak, aby platilo $0 \cdot x = b$.

13. ($\mathbb{Q}$, :), ($\mathbb{R}$, :)… není ani grupoid
dělení… ~~ND~~ $\wedge$ ~~K~~ $\wedge$ ~~A~~ $\wedge$ ~~EN~~ $\wedge$ ~~EI~~ $\wedge$ ~~ZR~~

14. ($\mathbb{Q}$ - {0}, ·), ($\mathbb{R}$ - {0}, ·)… komutativní grupa s neutrálním prvkem $e = 1$
násobení…ND $\wedge$ K $\wedge$ A $\wedge$ EN $\wedge$ EI $\wedge$ ZR

$$\bar{a} = \frac{1}{a}$$

D: $\overline{a\circ b} = \overline{a}\circ\overline{b}$

$$(a\circ b)\circ\overline{a\circ b} = e$$

$$(a\circ b)\circ(\overline{a}\circ\overline{b}) \overset{K}{=} (a\circ b)\circ(\overline{b}\circ\overline{a}) \overset{A}{=} [(a\circ b)\circ\overline{b}]\circ\overline{a} \overset{A}{=}$$

$$= [a\circ(b\circ\overline{b})]\circ\overline{a} = (a\circ e)\circ\overline{a} = a\circ\overline{a} = e$$

Odtud plyne, že $\overline{a\circ b} = \overline{a}\circ\overline{b}$, protože v komutativní grupě je inverzní prvek určen jednoznačně.

Obecná komutativní grupa $(M,\circ)$

$$\overline{\overline{a}} = a$$

$$\overline{a\circ b} = \overline{a}\circ\overline{b}$$

$$\overline{a\circ\overline{b}} = b\circ\overline{a}$$

$$a\circ c = b\circ c \Rightarrow a = b$$

Grupa $(C,+)$

$$-(-A) = A$$

$$-(A+B) = -A-B$$

$$-(A-B) = B-A$$

$$A+C = B+C \Rightarrow A = B$$

Grupa $(Q-\{0\},\cdot)$

$$(A^{-1})^{-1} = \frac{1}{\frac{1}{A}} = A$$

$$\frac{1}{A\cdot B} = \frac{1}{A}\cdot\frac{1}{B}$$

$$\left(\frac{A}{B}\right)^{-1} = \frac{1}{\frac{A}{B}} = \frac{B}{A}$$

$$A\cdot C = B\cdot C \Rightarrow A = B$$

VLASTNOSTI OPERACÍ URČENÝCH PŘEDPISEM

1 $(\mathbb{Z}, \circ)$ $x \circ y = x + y + 1$ — ND je zřejmé ($x, y \in \mathbb{Z} \Rightarrow x+y+1 \in \mathbb{Z}$)

K: $x \circ y = x + y + 1$
$y \circ x = y + x + 1$ vždy se rovná

A: $L = (x \circ y) \circ z = \underline{(x+y+1)} \circ \underline{z} = (x+y+1) + z + 1 = x + y + z + 2$ $L = P$
$P = x \circ (y \circ z) = \underline{x} \circ \underline{(y+z+1)} = x + (y+z+1) + 1 = x + y + z + 2$

EN: $x \circ e = x$
$x + e + 1 = x \quad | -x$
$\underline{e = -1}$

zk: $x \circ (-1) = x + (-1) + 1 = x$

EI: $x \circ \overline{x} = -1$
$x + \overline{x} + 1 = -1$
$\underline{\overline{x} = -x - 2}$

zk: $x \circ (-x-2) = x + (-x-2) + 1 = -1$

ZR: $a \circ x = b$
$a + x + 1 = b$
$\underline{x = b - a - 1}$

zk: $a \circ (b - a - 1) =$
$= a + (b - a - 1) + 1 =$
$= a + b - a - 1 + 1 = b$

ZR je vynuceno: $A \Rightarrow (EI \Leftrightarrow ZR)$
$1 \quad \boxed{1} \quad 1 \quad 1 \quad 1$

2 $(\mathbb{Z}, \circ)$ $x \circ y = x + y - 3$ — ND zřejmé

K: $x \circ y = x + y - 3$; $y \circ x = y + x - 3$ rovná se

A: $L = (x \circ y) \circ z = (x + y - 3) \circ z = (x + y - 3) + z - 3 = x + y + z - 6$ $L = P$
$P = x \circ (y \circ z) = x \circ (y + z - 3) = x + (y + z - 3) - 3 = x + y + z - 6$

EN: $x \circ e = x$
$x + e - 3 = x \quad | -x$
$\underline{e = 3}$

ZR: $a \circ x = b$
$a + x - 3 = b$
$\underline{x = b - a + 3}$

EI: $x \circ \overline{x} = 3$
$x + \overline{x} - 3 = 3$
$\underline{\overline{x} = -x + 6}$

komutativní grupa

③ $(N, *)$ $x * y = 2x - y$

~~ND~~ neplatí $x, y \in N$, ale $2x-y$ nemusí padnout do N
$(x = 1, y = 5)$

~~K~~; ~~A~~;

~~EN~~: $x * e = x$ $\quad$ $e * x = x$

$2x - e = x$ $\quad$ $2e - x = x$

$\underline{e = x}$ $\quad$ $\underline{e = x}$

e závisí na x!

~~EI~~:

~~ZR~~: $a * x = b$ $\quad$ $y * a = b$

$2a - x = b$ $\quad$ $2y - a = b$

$\underline{x = 2a - b}$ $\quad$ $y = \dfrac{a+b}{2}$

nemusí být přirozené číslo

④ $(Z, \circ)$ $x \circ y = x - 2y$

ND platí: x, y celá čísla $\Rightarrow$ $x - 2y$ je celé číslo

~~K~~: $x \circ y = x - 2y$ obecně se nerovná, např. $x = 3, y = 4$

$y \circ x = y - 2x$ $\quad$ $3 \circ 4 = -11$, $4 \circ 3 = -2$

~~A~~: $L = x \circ (y \circ z) = x \circ (y - 2z) = x - 2(y - 2z) = x - 2y + 4z$ $\quad$ $L \neq P$

$P = (x \circ y) \circ z = (x - 2y) \circ z = (x - 2y) - 2z = x - 2y - 2z$

~~EN~~: $x \circ e = x$ $\quad$ $e \circ x = x$

$x - 2e = x \mid -x$ $\quad$ $e - 2x = x$

$\underline{\underline{e = 0}}$ $\quad$ $\underline{e = 3x}$ e závisí na x

~~EI~~:

~~ZR~~: $a \circ x = b$ $\quad$ $y \circ a = b$ $\quad$ nekomutativní grupoid

$a - 2x = b$ $\quad$ $y - 2a = b$

$x = \dfrac{a-b}{2}$ $\quad$ $\underline{y = 2a + b}$

nemusí být celé číslo
$(a = 4, b = 1)$

5 $(\mathbb{Q}, \circ)$ $a \circ b = \dfrac{a+b}{2}$

ND platí $a, b \in \mathbb{Q} \Rightarrow \dfrac{a+b}{2} \in \mathbb{Q}$

K $L = a \circ b = \dfrac{a+b}{2}$ $L = P$

$P = b \circ a = \dfrac{b+a}{2}$

~~A~~: $L = (a \circ b) \circ c = \dfrac{a+b}{2} \circ c = \dfrac{\frac{a+b}{2} + c}{2} = \dfrac{a+b+2c}{4}$ $L \neq P$

$P = a \circ (b \circ c) = a \circ \dfrac{b+c}{2} = \dfrac{a + \frac{b+c}{2}}{2} = \dfrac{2a+b+c}{4}$

~~EN~~:

$a \circ e = a$ $e \circ a = a$

$\dfrac{a+e}{2} = a$ $\dfrac{e+a}{2} = a$

$a + e = 2a$ $e = a$

$e = a$

e závisí na a!

~~EI~~

ZR

$a \circ x = b$

$\dfrac{a+x}{2} = b$

$x = 2b - a \in \mathbb{Q}$

komutativní grupoid s vlastností ZR.

6

$(\mathbb{Q}, *)$ $a * b = 2ab$

ND platí $a, b \in \mathbb{Q} \Rightarrow 2ab \in \mathbb{Q}$

K platí $a * b = 2ab$, $b * a = 2ba$

A: $L = (a * b) * c = \underline{2ab} * \underline{c} = 2 \cdot (2ab) \cdot c = 4abc$ $L = P$

$P = a * (b * c) = \underline{a} * \underline{2bc} = 2 \cdot a \cdot (2bc) = 4abc$

EN: $a * e = a$

$2ae = a \mid : a, a \neq 0$

$e = \dfrac{1}{2}$

je-li $a \neq 0$, pak $e = \frac{1}{2}$;

je-li $a = 0$, pak $0 * \frac{1}{2} = 2 \cdot 0 \cdot \frac{1}{2} = 0$,

$0 * \frac{1}{2} = 0$

Číslo $\frac{1}{2}$ je neutrální prvek.

~~EI~~: $a * \bar{a} = \dfrac{1}{2}$

$2a\bar{a} = \dfrac{1}{2}$

$a\bar{a} = \dfrac{1}{4} \Rightarrow \bar{a} = \dfrac{1}{4a}$

pro $a = 0$ inverzní prvek neex. ~~neutr~~.

~~ZR~~: $A \Rightarrow (EI \Leftrightarrow ZR)$

$1 \; \boxed{1} \; 0 \; 1 \; \underline{0}$