OPERACE NA MNOŽINĚ

Def.: Nechť M je libovolná neprázdná množina, $n \in N$. Potom zobrazení $F: M^n \to M$, které každé uspořádané n-tici $(a_1, a_2, \dots, a_n) \in M^n$ přiřazuje nejvýše jeden prvek $a \in M$, nazýváme n-ární operací (operací četnosti n) na množině M.

Prvek $a \in M$, pro který platí $F(a_1, a_2, \dots, a_n) = a$, se nazývá obrazem n-tice $(a_1, a_2, \dots, a_n)$ v zobrazení F (výsledkem operace F provedené na prvky $a_1, a_2, \dots, a_n$).

Pro $n=1$ mluvíme o unární operaci, pro $n=2$ o binární operaci atd.

Dvojici (M, F), tj. množina M a operace F na ní, nazýváme algebraickou strukturou.

Budeme se zabývat binárními operacemi

PŘÍKLAD:

$(R, +)$, $(Q, :)$, $(P(M), \cap)$

$(R, +, \cdot)$, $(P(M), \cap, \cup)$

Poznámka: zápis binární operace

$F(a,b)$, $a * b$, $a \circ b$, $a \oplus b$, $a \bullet b$, ...

Binární operace na konečných množinách

→ Cayleyho tabulka [Arthur Cayley, 1821–1895]

PŘÍKLAD: Napište Cayleyho tabulku pro binární operaci $*$ na množině $M=\{0,1,2,3\}$: $a*b=z$, kde z je zbytek dělení $\frac{a+b}{4}$

(sčítání vzhledem k modulu 4)

PROBLÉM: Kolik různých operací můžeme definovat na množině M (na n-prvkové mn.)?

Def.: Algebraická struktura $(M,*)$ se nazývá

1. uzavřená na operaci $*$ (neomezeně definovaná) v M, jestliže $(\forall x,y\in M)(\exists z\in M)\ x*y=z$
2. asociativní v M, jestliže
   $(\forall x,y,z\in M)\ (x*y)*z = x*(y*z)$
3. s neutrálním prvkem, jestliže
   $(\exists e\in M)(\forall x\in M)\ e*x = x*e = x$
4. s inverzními prvky, jestliže má neutrální prvek $e\in M$ a platí:
   $(\forall x\in M)(\exists y\in M)\ x*y = y*x = e$
5. komutativní, jestliže
   $(\forall x,y\in M)\ x*y = y*x$

PROBLÉM: Jak poznáme uvedené vlastnosti z Cayleyho tabulky?

PŘÍKLAD: Vyšetřete vlastnosti daných operací, jsou-li a, b libovolná reálná čísla:

a) $a \oplus b = \frac{a+b}{2}$

b) $a \circ b = a+b+2$

? kolik neutrálních prvků může mít struktura

Věta: Každá struktura $(M,*)$ má nejvýše jeden neutrální prvek.

DK:

1. pokud $(M,*)$ nemá žádný n.p. věta platí
2. nechť $(M,*)$ má dva n.p. e_1, e_2

tj. $$\left.\begin{array}{l} e_1 * x = x * e_1 = x \rightarrow e_1 * e_2 = e_2 \\ e_2 * x = x * e_2 = x \rightarrow e_1 * e_2 = e_1 \end{array}\right\} e_1 = e_2$$

PŘÍKLAD: Je dána struktura $(M,*)$, kde $M=\{a,b,c,d\}$ a operace $*$ je určena Cayleyho tabulkou

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

Určete neutrální prvek a inverzní prvky této struktury

Poznámka: neutrální prvek značíme e

Věta: Nechť $(M,*)$ je asociativní struktura s neutrálním prvkem. Pak ke každému $x \in M$ existuje nejvýše jeden inverzní prvek $y \in M$.

DK:
Nechť y_1, y_2 jsou dva inv. prvky k x.

$x * y_1 = y_1 * x = e$
$\boxed{x * y_2} = y_2 * x = e$

$$y_1 = y_1 * e = y_1 * \boxed{(x * y_2)} \overset{\wedge}{=} (y_1 * x) * y_2 = e * y_2 = y_2$$

Poznámka: inverzní prvek k x budeme značit x^{-1}

Def.: Struktura $(M,*,\circ)$ se nazývá $(*,\circ)$-distributivní, právě když platí:

$$\forall x,y,z \in M;\ (x*y)\circ z = (x\circ z)*(y\circ z) \ \wedge$$
$$z\circ(x*y) = (z\circ x)*(z\circ y)$$

a nazývá se $(\circ,*)$-distributivní, právě když:

$$\forall x,y,z \in M;\ (x\circ y)*z = (x*z)\circ(y*z) \ \wedge$$
$$z*(x\circ y) = (z*x)\circ(z*y)$$

PŘÍKLAD: $(R,+,\cdot)$ je $(+,\cdot)$-distributivní, ale není $(\cdot,+)$-distributivní

PROBLÉM: Najděte strukturu, která je $(*,\circ)$ i $(\circ,*)$ distributivní.

ZÁKLADNÍ ALGEBRAICKÉ STRUKTURY

Def.: Nechť $(M,*)$ je algebraická struktura s jednou binární operací. Řekneme, že $(M,*)$ je

<u>GRUPOID</u>, pokud je $(M,*)$ uzavřená na $*$,

<u>POLOGRUPA</u>, pokud je $(M,*)$ asociativní grupoid,

<u>MONOID</u>, pokud je $(M,*)$ pologrupa s neutrálním prvkem,

<u>GRUPA</u>, pokud je $(M,*)$ monoid s inverzními prvky

<u>KOMUTATIVNÍ (ABELOVA) GRUPA</u>, pokud je $(M,*)$ grupa a operace $*$ je komutativní.

PŘÍKLADY:

grupoid $(\mathbb{Z},-)$

pologrupa $(\mathbb{Q}^+,+)$

monoid $(L,\cdot)$, L ... mn. všech lichých čísel

grupa $(P,\circ)$, P ... mn. všech prostých zobrazení

komutativní grupa

$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$

$(\mathbb{Q}-\{0\},\cdot)$, $(\mathbb{R}-\{0\},\cdot)$, $(K-\{0\},\cdot)$

$(M,\oplus)$ ... $\oplus$ je operace „sčítání na hod. ciferníku"

PŘÍKLAD: $(A, \oplus)$, $A = \{0,1,2\}$

$\oplus$ ... sčítání podle modulu 3

D.ú. tj. $a \oplus b = z$, z je zbytek při $(a+b):3$

Ukažte, že $(A, \oplus)$ je Abelova grupa

PROBLÉM: Nechť $(M,*)$ je grupa. Dokažte, že platí:

a) $\forall x,y,z \in M$; $(x*y)^{-1} = y^{-1} * x^{-1}$

b) $x*z = y*z \Rightarrow x = y$

DK:

ad a) $(x*y)*(x*y)^{-1} = (x*y)*(y^{-1}*x^{-1}) = x*(y*y^{-1})*x^{-1} = \dots$

ad b) $x*z = y*z \Rightarrow x*z*z^{-1} = y*z*z^{-1} \Rightarrow \dots$

TĚLESO

$(R,+,\cdot)$
- $(R,+)$ komutativní grupa
- $(R-\{0\},\cdot)$ (komutativní) grupa

Def.: Struktura $(M,*,\circ)$ s alespoň dvěma prvky se nazývá těleso, právě když je $(*,\circ)$-distributivní, když struktura $(M,*)$ je komutativní grupa a když $(M\setminus\{0\},\circ)$, kde 0 je neutrální prvek grupy $(M,*)$, je grupa. Je-li navíc $(M\setminus\{0\},\circ)$ komutativní nazýváme $(M,*,\circ)$ komutativním tělesem. Neutrální prvek 0 grupy $(M,*)$ se nazývá nulový prvek tělesa M a neutrální prvek 1 grupy $(M\setminus\{0\},\circ)$ se nazývá jednotkový prvek těl. F