Algebraické struktury

Def. (Kartézský součin): Kartézským součinem množin A a B nazveme množinu:

$$A \times B = \{(a,b) \mid a \in A \,.\, b \in B\}$$

Pozn.: Tzn. $A \times B$ je množina všech uspořádaných dvojic (a,b) kde $a \in A$ a $b \in B$.

Úmluva: Značením $f : A \to B$ máme dále na mysli zobrazení jehož definičním oborem je A. Pokud ne, bude to řečeno.

Def. (Binární operace): Binární operací na množině A nazveme každé zobrazení $\circ : A \times A \to A$.

Př.: 1.) $A = \mathbb{N}$... množina přirozených čísel

$\circ = +$ ... sčítání přirozených čísel

$\Rightarrow$ například $\circ(3,4) = 3+4 = 7$

obvyklé místo zápisu $\circ(a,b)$ píšeme $a \circ b$

Víme, že součet dvou přirozených čísel je opět přirozené číslo $\Rightarrow$

$\forall a,b \in \mathbb{N}: \quad a \circ b \in \mathbb{N} \Rightarrow \circ$ je zobrazení z $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$\Rightarrow$ $\circ$ je binární operací na $\mathbb{N}$.

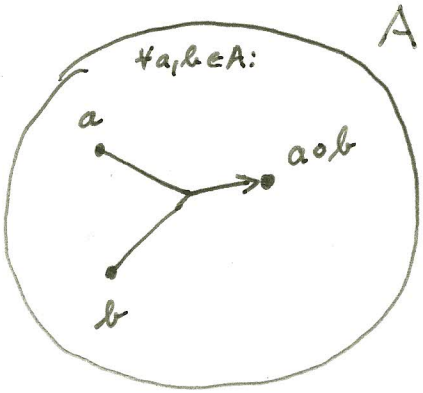
2.) $A = \mathbb{N}$... množina přirozených čísel

$\circ$... je dáno předpisem: $\forall a,b \in \mathbb{N}: a \circ b = \frac{a}{b} \Rightarrow$

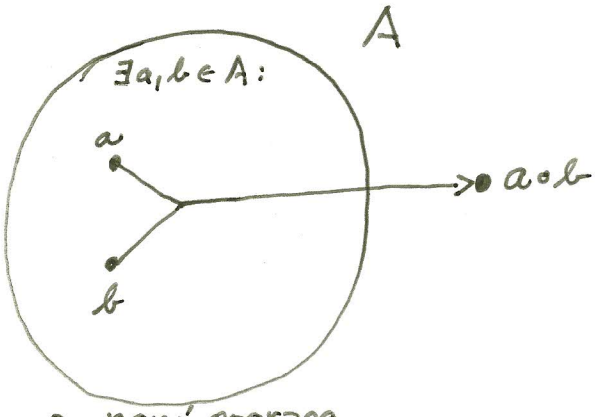
$\Rightarrow$ například $4 \circ 2 = \frac{4}{2} = 2 \in \mathbb{N}$, ale $3 \circ 4 = \frac{3}{4} \notin \mathbb{N} \Rightarrow$

$\circ$ není binární operace na $\mathbb{N}$

$\Rightarrow$



$\circ$ je operace



$\circ$ není operace

Def (Grupoid): Uspořádanou dvojici $(A, \circ)$, kde A je neprázdná množina a $\circ$ je operace na A, nazveme grupoidem.

Př:
1.) $(\mathbb{N}, +)$ = je grupoid

2.) $(I, \cdot)$, kde I je množina iracionálních čísel
. je restrikce násobení reálných čísel na I

$\Rightarrow$ $\underset{\uparrow I}{\sqrt{2}} \cdot \underset{\uparrow I}{\sqrt{2}} = 2 \notin I$ $\Rightarrow$. není operace na I $\Rightarrow$ $(I, \cdot)$ není grupoid

Def (Pologrupa): Uspořádanou dvojici $(A, \circ)$, kde A je neprázdná množina a $\circ$ je zobrazení definované na $A \times A$ splňující:

1.) $\forall a, b \in A : a \circ b \in A$ (uzavřenost $\Rightarrow$ je to grupoid)

2.) $\forall a, b, c \in A : a \circ (b \circ c) = (a \circ b) \circ c$ (asociativita)

nazveme pologrupou.

Př.: I.) $(\mathbb{Z}, +)$ (obvyklé sčítání na $\mathbb{Z}$) je pologrupa, protože

1.) $\forall a, b \in \mathbb{Z} : \quad a + b \in \mathbb{Z}$

2.) $\forall a, b, c \in \mathbb{Z} : \quad (a+b)+c = a+(b+c)$

II.) $(F_1, \circ)$, kde

$F_1 = \{ f : \mathbb{R} \to \mathbb{R} \mid f(1) = 1 \}$, $\circ$ ... skládání zobrazení

1.) uzavřenost: $\forall f, g \in F_1 : (f \circ g)(1) = f(g(1)) = f(1) = 1 \Rightarrow$

$\Rightarrow (f \circ g)(1) = 1 \Rightarrow f \circ g \in F_1 \Rightarrow$ splněno!

2.) asociativita: Skládání zobrazení je asociativní:

$\forall f, g, h \in F_1 : [f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x)))$

$[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x)))$

Def. (Neutrální prvek): Nechť $\circ$ je operace na A. Prvek $e \in A$ nazveme neutrálním prvkem vzhledem k operaci $\circ$ právě tehdy, když

$$\forall a \in A : \quad a \circ e = e \circ a = a$$

Př.: 1.) $(\mathbb{R}, \cdot) \Rightarrow e = 1$

2.) $(\mathbb{R}, +) \Rightarrow e = 0$

Def. (Monoid): Uspořádanou dvojici $(A, \circ)$, kde A je neprázdná množina a $\circ$ je zobrazení definované na $A \times A$ nazveme monoid právě když

1.) $\forall a, b \in A: \quad a \circ b \in A$

2.) $\forall a, b, c \in A: \quad (a \circ b) \circ c = a \circ (b \circ c)$

3.) $\exists e \in A \; \forall a \in A: \quad a \circ e = e \circ a = a$

Př. 1.) $(M_{(n,n)}, \cdot)$

$M_{(n,n)}$ .... matice řádu (n, n)

$\cdot$ ... násobení matic

1.) $\forall A, B \in M_{(n,n)}: \quad A \cdot B \in M_{(n,n)}$

2.) $\forall A, B, C \in M_{(n,n)}: \quad (A \cdot B) \cdot C = A \cdot (B \cdot C)$

3.) $\exists E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in M_{(n,n)} \; \forall A \in M_{(n,n)}: \quad A \cdot E = E \cdot A = A$

$\Rightarrow$ $(M_{(n,n)}, \cdot)$ je monoid

2.) $(F_{\mathbb{R}}, \circ)$

$F_{\mathbb{R}} = \{ f : \mathbb{R} \to \mathbb{R} \mid \mathcal{D}_f = \mathbb{R} \}$

$\circ$ ... skládání zobrazení

1.) $\forall f, g \in F_{\mathbb{R}}: \quad (\forall x \in \mathbb{R} \; \exists g(x) \in \mathbb{R}) \Rightarrow (\forall x \in \mathbb{R} \; \exists f(g(x))) \Rightarrow f \circ g \in F_{\mathbb{R}}$

2.) Skládání zobrazení je asociativní

3.) $\exists e \in F_{\mathbb{R}}$, kde $\forall x \in \mathbb{R}: e(x) = x$ a $\forall f \in F_{\mathbb{R}}:$

$(f \circ e)(x) = f(e(x)) = f(x) \Rightarrow f \circ e = f$

$(e \circ f)(x) = e(f(x)) = f(x) \Rightarrow e \circ f = f$

$\Rightarrow (F_{\mathbb{R}}, \circ)$ je monoid

Věta (O jednoznačnosti neutrálního prvku): Nechť $(A, \circ)$ je grupoid. Jestliže v A existuje nějaký neutrální prvek vzhledem k operaci $\circ$, pak je jediný.

Důkaz: Nechť e_1 a také e_2 je neutrálním prvkem vzhledem k $\circ$.

$$\Rightarrow \quad e_1 = e_1 \circ e_2 = e_2 .$$

□

Důsledek: V monoidu $(A, \circ)$ existuje právě jeden neutrální prvek.

Def. (Inverzní prvek): Nechť $(A, \circ)$ je grupoid a $e \in A$ je neutrální prvek vzhledem k $\circ$. Prvkem inverzním k prvku a vzhledem k operaci $\circ$ nazveme prvek $\bar{a}^{-1} \in A$ splňující:

$$a \circ \bar{a}^{-1} = \bar{a}^{-1} \circ a = e$$

Př.: 1.) $(\mathbb{R}, .) \Rightarrow (\bar{2})^{-1} = \frac{1}{2}$, $(\bar{3})^{-1} = \frac{1}{3}$, ale $(\bar{0})^{-1}$ neexistuje

2.) $(\mathbb{R}, +) \Rightarrow (\bar{2})^{-1} = -2$, neboť $2 + (-2) = 0 = e$

$(\bar{-3})^{-1} = +3$, neboť $(-3) + (3) = 0 = e$

Def. (Grupa): Uspořádanou dvojici $(A, \circ)$, kde A je neprázdná množina a $\circ$ je zobrazení definované na $A \times A$ nazveme grupou právě když:

je to grupoid $\Leftarrow$ 1.) $\forall a, b \in A : a \circ b \in A$ (uzavřenost)

je to pologrupa $\Leftarrow$ 2.) $\forall a, b, c \in A : (a \circ b) \circ c = a \circ (b \circ c)$ (asociativita)

je to monoid $\Leftarrow$ 3.) $\exists e \in A \; \forall a \in A : a \circ e = e \circ a = a$ (existence neutr. prvku)

4.) $\forall a \in A \; \exists \bar{a}^1 \in A : a \circ \bar{a}^1 = \bar{a}^1 \circ a = e$ (exist. neutrálních prvků)

Příklad: $(P, \circ)$, kde $P = \{ f : \mathbb{R} \to \mathbb{R} \mid \mathcal{D}_f = H_f = \mathbb{R}, f \text{ je prostá funkce} \}$ a $\circ$ je skládání funkcí, tvoří grupu:

1.) $\forall f, g \in P$: $\mathcal{D}_{f \circ g} = \mathbb{R}$ a platí: $(f \circ g)(x_1) = (f \circ g)(x_2) \Rightarrow f(g(x_1)) = f(g(x_2)) \Rightarrow g(x_1) = g(x_2) \Rightarrow x_1 = x_2$

$\Rightarrow f \circ g$ je prostá funkce $\Rightarrow f \circ g \in P$

2.) Skládání zobrazení je asociativní.

3.) Neutrálním prvkem vzhledem ke skládání je identita $id(x) = x \Rightarrow id \in P$

4.) K funkci prosté existuje fce inverzní $\Rightarrow \forall f \in P \; \exists \bar{f}^1 \in P : f \circ \bar{f}^1 = \bar{f}^1 \circ f = id$ ($D(f^{-1}) = H(f) = \mathbb{R}$)

(a je to také prostá funkce!)

□

Věta (O jednoznačnosti inverzního prvku): Nechť $(A, \circ)$ je grupa. Potom ke každému prvku existuje právě jeden prvek inverzní. Tzn.:

$$\forall a \in A \; \exists! \, \bar{a}^1 \in A : a \circ \bar{a}^1 = \bar{a}^1 \circ a = e.$$

Důkaz: Předpokládejme, že $\bar{a}_1^1$ i $\bar{a}_2^1$ jsou prvky inverzní k $a \in A \Rightarrow$

$$\bar{a}_1^1 = \bar{a}_1^1 \circ e = \bar{a}_1^1 \circ (a \circ \bar{a}_2^1) = (\bar{a}_1^1 \circ a) \circ \bar{a}_2^1 = e \circ \bar{a}_2^1 = \bar{a}_2^1$$

□

Věta (O inverzi inverze): Nechť $(G,\circ)$ je grupa. Potom

$$\forall a \in G : (\bar{a}^1)^{-1} = a$$

Důkaz: $(G,\circ)$ je grupa $\Rightarrow \forall a \in G \; \exists \bar{a}^1 \in G : \bar{a}^1 \circ a = a \circ \bar{a}^1 = e \Rightarrow (\bar{a}^1)^{-1} = a$ □

Věta (O krácení v grupě): Nechť $(G,\circ)$ je grupa. Potom $\forall a,b,c \in G$:

1.) $(a \circ c = b \circ c) \Rightarrow (a = b)$

2.) $(c \circ a = c \circ b) \Rightarrow (a = b)$

Důkaz: V grupě existuje neutrální prvek $e \in G$ a také $\bar{c}^1$. Proto platí:

ad 1.) $(a \circ c = b \circ c) \Rightarrow a = a \circ e = \overbrace{a \circ c}^{b \circ c} \circ \underbrace{c \circ \bar{c}^1}_{e} = b \circ \underbrace{c \circ \bar{c}^1}_{e} = b \circ e = b$

ad 2.) $(c \circ a = c \circ b) \Rightarrow a = e \circ a = \bar{c}^1 \circ c \circ a = \bar{c}^1 \circ c \circ b = e \circ b = b$ □

Věta: Nechť $(G,\circ)$ je grupa, $g \in G$ a e je neutrální prvek v $(G,\circ)$.

1.) Jestliže $\exists g^* \in G : g^* \circ g = e$, pak $g^* = \bar{g}^1$.

2.) Jestliže $\exists g^* \in G : g \circ g^* = e$, pak $g^* = \bar{g}^1$.

Důkaz: ad 1.)

$g = g \circ e$

$g = g \circ (g^* \circ g)$ (předpoklad $g^* \circ g = e$)

$e \circ g = (g \circ g^*) \circ g$ (věta o krácení)

$e = g \circ g^*$

$\Rightarrow g^* \circ g = g^* \circ g = e \Rightarrow g^* = \bar{g}^1$

ad 2.)

$g = e \circ g$

$g = (g \circ g^*) \circ g$

$g \circ e = g \circ (g^* \circ g)$ /krácení

$e = g^* \circ g$

$\Rightarrow g \circ g^* = g^* \circ g = e$

Věta: Nechť $(G,\circ)$ je grupa, $e \in G$ je neutrálním prvkem vzhledem k $\circ$.

1.) Jestliže $\exists g \in G\ \exists a \in G: a \circ g = a$, pak $g = e$

2.) Jestliže $\exists g \in G\ \exists a \in G: g \circ a = a$ pak $g = e$

Důkaz:

ad 1.) $\forall a \in G: a \circ g = a \Rightarrow e = \underbrace{\bar{a}^{-1} \circ a}_{\text{jistě existuje, neboť } (G,\circ) \text{ je grupa}} = \bar{a}^{-1} \circ (a \circ g) = e \circ g = g$

ad 2.) $\forall a \in G: g \circ a = a \Rightarrow e = a \circ \bar{a}^{-1} = (g \circ a) \circ \bar{a}^{-1} = g \circ e = g$ □

Poznámka: Při ověřování, zda $g \in G$ je neutrálním prvkem v grupě $(!)$ $(G,\circ)$ stačí ověřit, že $\exists a \in G: a \circ g = a$, rovnost $g \circ a = a$ je pak již zajištěna a není ji třeba ověřovat.

Věta: Nechť $(A,\circ)$ je grupa i $a_1, a_2, \dots, a_m \in A$. Potom platí

$$(a_1 \circ a_2 \circ \dots \circ a_m)^{-1} = \bar{a}_m^{-1} \circ \dots \circ \bar{a}_2^{-1} \circ \bar{a}_1^{-1}$$

Důkaz: z asociativity $\circ$ plyne:

a) $(a_1 \circ a_2 \circ \dots \circ a_m) \circ (\bar{a}_m^{-1} \circ \dots \circ \bar{a}_2^{-1} \circ \bar{a}_1^{-1}) =$

$= a_1 \circ a_2 \circ \dots \circ \underbrace{(a_m \circ \bar{a}_m^{-1})}_{e} \circ \dots \circ \bar{a}_2^{-1} \circ \bar{a}_1^{-1} =$

$= a_1 \circ a_2 \circ \dots \circ \underbrace{a_{m-1} \circ \bar{a}_{m-1}^{-1}}_{e} \circ \dots \circ \bar{a}_2^{-1} \circ \bar{a}_1^{-1} =$

$\vdots$

$= a_1 \circ \bar{a}_1^{-1} = e$

b) $(\bar{a}_m^{-1} \circ \dots \circ \bar{a}_2^{-1} \circ \underbrace{\bar{a}_1^{-1}}_{e}) \circ (a_1 \circ a_2 \circ \dots \circ a_m) = \dots = e$

□