Binární operace

Definice: *Binární operace* na množině X je zobrazení $X \times X \to X$.

Příklady: Na $\mathbb{R}$ jsou $+$, $-$ a $\cdot$ binární operace; zápis $(\mathbb{R}, +)$ apod.

Podíl : je binární operací na $\mathbb{R} \setminus 0$, případně na $\mathbb{R}^+$ ale nikoli na $\mathbb{R}$. Formálně je podíl na $\mathbb{R}$ zobrazení $\mathbb{R} \times (\mathbb{R} \setminus 0) \to \mathbb{R}$. Lze ho zúžit na $\mathbb{R} \setminus 0$ nebo na $\mathbb{R}^+$. Rozšíření o dělení 0 má nesmyslné důsledky.

Na $\mathbb{N}$ jsou $+$ a $\cdot$ binární operace, ale $-$ binární operace na $\mathbb{N}$ není.

Maticový součet je binární operace na maticích stejného řádu.

Součin je binární operace na *čtvercových* maticích stejného řádu.

$(a, b) \to a^2 - b + 18$ je binární operace na $\mathbb{R}$ a $\mathbb{Z}$, ale ne na $\mathbb{N}$.

$(a, b) \to b$ je binární operace na libovolné množině.

$(p, q) \to r$, kde $\forall x \in \mathbb{R} : r(x) = p(x) + q(x)$, je binární operace na množině reálných funkcí $\mathbb{R}[x]$, píšeme $r = p + q$.

Binární operaci na konečné množině lze popsat tabulkou.

$(a, b) \to \neg a \wedge b$

	0	1
0	0	1
1	0	0

Grupa

Definice: *Grupa* $(G, \circ)$ je množina G spolu s binární operací $\circ$ na G splňující následující axiomy:

- $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$
  ... operace $\circ$ je *asociativní*,
- $\exists e \in G \; \forall a \in G : a \circ e = e \circ a = a$
  ... e se nazývá *neutrální prvek*,
- $\forall a \in G \; \exists b \in G : a \circ b = b \circ a = e$
  ... b se nazývá *inverzní prvek* k prvku a, značíme jej a^{-1}

Pokud je navíc operace $\circ$ *komutativní*, t.j. $\forall a, b \in G : a \circ b = b \circ a$, potom se $(G, \circ)$ nazývá *Abelovská* grupa.

Ukázky: Nejmenší grupa je $(\{e\}, \circ)$, kde $e \circ e = e$.

Pro $G = \{e, a, b\}$ a $\circ$ definovanou tabulkou dostáváme grupu $(G, \circ)$, kde e je neutrální prvek, e je inverzní sám k sobě, a prvky a a b jsou navzájem inverzní. Tato grupa je Abelovská.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Fakt: Nejmenší neabelovská grupa S_3 má 6 prvků.

Aditivní a multiplikativní grupy

Grupy $(G, \circ)$, kde $\circ$ je odvozena od sčítání se nazývají *aditivní*, například $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}[x], +)$, $(\mathbb{R}^{m\times n}, +)$. Tyto příklady jsou Abelovské. $(\mathbb{N}, +)$ není grupa.

Na aditivních grupách se neutrální prvek nazývá *nulový prvek* nebo *nula* a značí se 0, $\mathbf{0}$, $\mathbf{0}_{m,n}$ apod.
Inverznímu prvku se často říká *opačný* a namísto a^{-1} se značí $-a$.
Lze zavést binární operaci *rozdíl* jako součet s opačným prvkem, formálně: $a - b = a + (-b)$.

Multiplikativní grupy mají $\circ$ odvozenu od součinu, například abelovské $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\{-1, 1\}, \cdot)$ a $(\{z \in \mathbb{C} : |z| = 1\}, \cdot)$.

Regulární matice řádu n se součinem tvoří grupu, která ovšem *není Abelovská*. Neutrální prvek je $\mathbf{I}_n$. Inverzní prvek k $\boldsymbol{A}$ je $\boldsymbol{A}^{-1}$.

V multiplikativních grupách se neutrální prvek někdy značí 1.
Podobně lze definovat *podíl* jako $a : b = a \cdot b^{-1}$.

Vlastnosti grup

Pozorování: Neutrální prvek je jednoznačně určen.

Důkaz: Pokud by e a e' byly oba neutrální, pak $e = e \circ e' = e'$.

Pozorování: Každé a jednoznačně určuje svůj inverzní prvek a^{-1}.

Důkaz: Pokud by b a b' byly oba inverzní k a, pak
$b = b \circ e = b \circ (a \circ b') = (b \circ a) \circ b' = e \circ b' = b'$.

Pozorování: Ekvivalentní úpravy jsou:
$a = b \;\Leftrightarrow\; a \circ c = b \circ c \;\Leftrightarrow\; c \circ a = c \circ b$

Důkaz: $\Rightarrow$ triv., $\Leftarrow$: $a = a \circ e = a \circ c \circ c^{-1} = b \circ c \circ c^{-1} = b \circ e = b$

Pozorování: Rovnice $a \circ x = b$ a $y \circ a = b$ mají jednoznačná řešení.

Důkaz: $x = e \circ x = a^{-1} \circ a \circ x = a^{-1} \circ b$; analogicky $y = b \circ a^{-1}$.

Cvičení: Dokažte sami: $(a^{-1})^{-1} = a$, $\quad (a \circ b)^{-1} = b^{-1} \circ a^{-1}$,
$a \neq b \;\Rightarrow\; a^{-1} \neq b^{-1}$.

Kvíz — řešení

Je-li u některých otázek více možností správných, vyberte všechny.

1. Které z logických operací tvoří grupu na množině $\{0, 1\}$?
   a) $\neg$ b) $\wedge$ c) $\vee$ d) $\Rightarrow$ e) $\Leftrightarrow$
2. Pravda nebo lež?
   Každá komutativní binární operace je asociativní.

Pro $n \in \mathbb{N}$ nechť $a^n = \underbrace{a \circ a \circ \cdots \circ a}_{n\times}$ a $a^{-n} = \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n\times}$.

3. Která z následujících pravidel platí pro $a, b \in G$, $m, n \in \mathbb{N}$ ve všech grupách a která nikoli?
   a) $a^{m+n} = a^m \circ a^n$ b) $(a \circ b)^n = a^n \circ b^n$ c) $(a^n)^{-1} = a^{-n}$
4. Pokud $a^n = b$, kolik je a^{2n}?
   a) e b) b c) $2b$ d) $b \circ b$ e) e^n f) b^n

Komentář k řešení kvízu

1. Operace $\neg$ není binární; $\wedge$, $\vee$ nemají inverzní prvky;
   $\Rightarrow$ nemá už ani neutrální prvek;
   $\Leftrightarrow$ neutrální prvek je 1 a oba prvky jsou samy sobě inverzní.
2. Např. $a \circ b = 2^{a+b}$ je komutativní, ale nikoli asociativní.
3. a) $\underbrace{a \circ a \circ \cdots \circ a}_{(m+n)\times} = \underbrace{a \circ a \circ \cdots \circ a}_{m\times} \circ \underbrace{a \circ a \circ \cdots \circ a}_{n\times}$

   b) platí jen pro komutativní operace, obecně nikoli
   $(a \circ b)^n = \underbrace{a \circ b \circ a \circ \cdots \circ b}_{\text{střídavě } n\times a,\ n\times b} \neq \underbrace{a \circ \cdots \circ a}_{n\times} \circ \underbrace{b \circ \cdots \circ b}_{n\times} = a^n \circ b^n$

   c) $a^n \circ a^{-n} = \underbrace{a^{n-1} \circ a}_{a^n} \circ \underbrace{a^{-1} \circ a^{1-n}}_{a^{-n}} = a^{n-1} \circ e \circ a^{1-n} =$

   $a^{n-1} \circ a^{1-n} = a^{n-2} \circ a^{2-n} = \cdots = a \circ a^{-1} = e$.
4. $a^{2n} = \underbrace{a \circ \cdots \circ a}_{2n\times} = \underbrace{a \circ \cdots \circ a}_{n\times} \circ \underbrace{a \circ \cdots \circ a}_{n\times} = a^n \circ a^n = b \circ b$.

   Zatímco $b \circ b = b^2$, nemá výraz $2b$ v grupě s operací $\circ$ smysl.

Otázky k porozumění tématu přednášky

- V literatuře bývají někdy uváděny tzv axiomy *uzavřenosti*, např. $\forall a, b \in G : a \circ b \in G$. Proč tyto axiomy neuvádíme?
- Lze axiom o existenci inverzního prvku zkrátit na $\forall a \in G\ \exists b \in G : a \circ b = e$ a vztah $b \circ a = e$ z něj odvodit podobně jako ve tvrzení o inverzní matici?
- Lze stejně zjednodušit axiom o neutrálním prvku?
- Které vlastnosti binárních operací zaručují korektnost ekvivalentních úprav rovnic na grupě?