POLOGRUPY, MONOIDY, GRUPY

BINÁRNÍ OPERACE na množině A je libovolné zobrazení $A \times A \longrightarrow A$.

Př.: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(m, n) \longmapsto m + n$$

Binární operace $*$ na množině A je ASOCIATIVNÍ, jestliže pro každé tři prvky $a, b, c \in A$ platí

$$a * (b * c) = (a * b) * c.$$

Binární operace $*$ na množině A je KOMUTATIVNÍ, jestliže pro každé dva prvky $a, b \in A$ platí

$$a * b = b * a$$

Pologrupy

Buď A množina, $*$ binární operace na množině A, která je asociativní. Potom dvojice $(A, *)$ se nazývá POLOGRUPA.
Pologrupa $(A, *)$ se nazývá KOMUTATIVNÍ, jestliže $*$ je komutativní operace.

Příklady
- $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
- $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$
- množina matic stejného typu se sčítáním
- množina polynomů se sčítáním

$\vdots$

Monoidy

Buď $*$ binární operace na množině A.
Prvek $e \in A$ se nazývá NEUTRÁLNÍ prvek vzhledem k operaci $*$, jestliže pro každý prvek $a \in A$ platí

$$a * e = e * a = a.$$

Tvrzení V množině A s binární operací $*$ existuje nejvýše jeden neutrální prvek.

Důkaz Buďte e', e'' neutrální prvky operace $*$.
Pak $e'' = e' * e'' = e'$.

Buď $(A, *)$ pologrupa s neutrálním prvkem e.
Trojice $(A, *, e)$ se nazývá MONOID.

Monoid $(A, *, e)$ se nazývá KOMUTATIVNÍ, jestliže pologrupa $(A, *)$ je komutativní.

Příklady
- $(\mathbb{Z}, +, 0)$, $(\mathbb{R}, +, 0)$, ...
- $(\mathbb{N}, \cdot, 1)$, $(\mathbb{R}, \cdot, 1)$, $(\mathbb{C}, \cdot, 1)$, ...
- množina matic se sčítáním a nulovou maticí
- množina matic s násobením a jednotkovou maticí

⋮

Grupy

Buď $(A,*,e)$ monoid. Prvek $a \in A$ se nazývá INVERTIBILNÍ, jestliže existuje prvek $b \in A$ takový, že $a*b=b*a=e$.

Prvek b se nazývá INVERZNÍ k prvku a.

Tvrzení Buď $(A,*,e)$ monoid. Je-li prvek $a \in A$ invertibilní, pak k němu existuje právě jeden prvek inverzní.

Důkaz Buďte $b', b'' \in A$ inverzní prvky k $a \in A$. Tedy, $b'*a=a*b'=e=b''*a=a*b''$.

Pak $b'=b'*e=b'*(a*b'')=(b'*a)*b''=$

$=e*b''=b''$. $\square$

Monoid, jehož každý prvek je invertibilní, se nazývá GRUPA. Píšeme $(A,*,e,^{-1})$.

Příklady • $(\mathbb{Z},+,0,-)$, $(\mathbb{R},+,0,-)$, ...

• $(\mathbb{Q}\setminus\{0\},\cdot,1,^{-1})$, $(\mathbb{R}\setminus\{0\},\cdot,1,^{-1})$, ...

Lemma Buď $(G,*,1,^{-1})$ grupa. Pak pro libovolná $a,b \in G$ platí:

1) jestliže $a*b=1$, pak $b=a^{-1}$, $a=b^{-1}$.

2) $1^{-1}=1$.

3) $(a^{-1})^{-1}=a$.

4) $(a*b)^{-1}=b^{-1}*a^{-1}$.

Podpologrupy

Buď $(A, *)$ pologrupa, buď $B \subseteq A$. Nechť platí

jestliže $b_1, b_2 \in B$, pak $b_1 * b_2 \in B$.

Potom B se nazývá PODPOLOGRUPA pologrupy A.

Příklady
- $(\mathbb{N}, +) \subset (\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset$
  $\subset (\mathbb{C}, +)$
- $(\mathbb{N}, \cdot) \subset (\mathbb{Z}, \cdot) \subset \ldots$

Podmonoidy

Buď $(A, *, e)$ monoid, buď $B \subseteq A$. Nechť platí

1) jestliže $b_1, b_2 \in B$, pak $b_1 * b_2 \in B$.

2) $e \in B$.

Potom B se nazývá PODMONOID monoidu A.

Podgrupy

Buď $(A, *, e, ^{-1})$ grupa, $B \subseteq A$. Nechť

1) jestliže $b_1, b_2 \in B$, pak $b_1 * b_2 \in B$

2) $e \in B$.

3) jestliže $b \in B$, pak $b^{-1} \in B$.

Potom B se nazývá PODGRUPA grupy A.

<u>Podgrupy aditivní grupy $\mathbb{Z}$</u>

$(\mathbb{Z}, +, 0, -)$.

Pro $m \in \mathbb{N}$ označme

$$m\mathbb{Z} = \{m \cdot k \mid k \in \mathbb{Z}\} = \{\dots, -3m, -2m, -m, 0, m, 2m, \dots\}$$

<u>Tvrzení</u> Podmnožiny $m\mathbb{Z} \subseteq \mathbb{Z}$ jsou podgrupy v grupě $\mathbb{Z}$ a jiné podgrupy v grupě $\mathbb{Z}$ nejsou.