POLOGRUPY, MONOIDY, GRUPY

BINÁRNÍ OPERACE na množině A je zobrazení $A \times A \to A$.

Binární operace $*$ na množině A je ASOCIATIVNÍ, když pro každé 3 prvky $a, b, c \in A$ platí

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

Binární operace $*$ na množině A je KOMUTATIVNÍ, když pro každé 2 prvky $a, b \in A$ platí

$$a * b = b * a.$$

Množina A s asociativní binární operací $*$ je POLOGRUPA. Zapisujeme $(A, *)$.

Pokud $*$ je komutativní, nazývá se pologrupa $(A, *)$ KOMUTATIVNÍ.

Př.: $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$

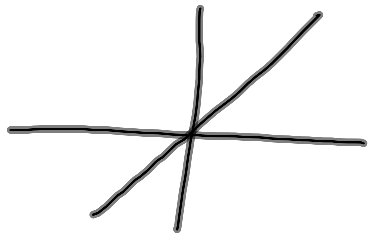
Př.: X nepr. množina. X^X mn. všech zobrazení $X \to X$. Vezmeme operaci $\circ$. $(X^X, \circ)$ je pologrupa.

Buď $*$ bin. operace na mn. A. Prvek $e \in A$ je NEUTRÁLNÍ PRVEK vzhledem k $*$, jestliže pro každý prvek $a \in A$ platí

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

Př: $A = \mathbb{R}^{\mathbb{R}}$, $* = \circ$

$e : \mathbb{R} \to \mathbb{R}$, $e(x) = x$, $e = id_{\mathbb{R}}$



$f : \mathbb{R} \to \mathbb{R}$

$$(f \circ id_{\mathbb{R}})(x) = f(id_{\mathbb{R}}(x)) = f(x)$$

$$(id_{\mathbb{R}} \circ f)(x) = id_{\mathbb{R}}(f(x)) = f(x)$$

<u>Tvrzení</u> V množině A se zadanou bin. operací $*$ existuje nejvýše jeden neutrální prvek.

<u>Důkaz</u> e', e'' neutrální prvky. $\forall a \in A$ platí $e' * a = a * e' = a$, $e'' * a = a * e'' = a$.

$$e'' = e' * e'' = e'.$$

Pologrupa $(A, *)$ s neutrálním prvkem e je MONOID. Zapisujeme $(A, *, e)$. Pokud $*$ je komutativní, je monoid $(A, *, e)$ KOMUTATIVNÍ.

Buď $(A,*,e)$ monoid. Prvek $a\in A$ je INVERTIBILNÍ, když existuje prvek $b\in A$ takový, že $a*b=b*a=e$.
Prvek b je INVERZNÍ k a.

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

__Důkaz__ Existence vyplývá z toho, že a je invertibilní.
Předp., že b', b'' jsou inverzní prvky k a.

$$a*b'=b'*a=e\ ,\quad e*b''=b''*a=e.$$

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

Monoid, jehož každý prvek je invertibilní, je GRUPA.

Př.: $(\mathbb{Z},+,0,-)$, $(\mathbb{R},+,0,-)$, $(\mathbb{R}\setminus\{0\},\cdot,1,{}^{-1})$

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

1) $a*b=1 \Rightarrow b=a^{-1},\ a=b^{-1}$.
2) $1^{-1}=1$
3) $(a^{-1})^{-1}=a$
4) $(a*b)^{-1}=b^{-1}*a^{-1}$

__Důkaz__ 1) $a*b=1 \Rightarrow b=1*b=a^{-1}*a*b=a^{-1}*1=a^{-1}$.

2) $1*1=1$

3) $a^{-1}*a=1$

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

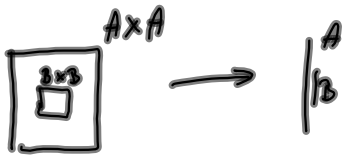
PODSTRUKTURY

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

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

Pak B se nazývá PODPOLOGRUPA pologrupy A.

$*: A \times A \to A$



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

1) $b_1, b_2 \in B \Rightarrow b_1 * b_2 \in B$

2) $e \in B$.

Potom B se nazývá PODMONOID monoidu A.

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

1) $b_1, b_2 \in B \Rightarrow b_1 * b_2 \in B$

2) $e \in B$

3) $b \in B \Rightarrow b^{-1} \in B$.

Pak B je PODGRUPA grupy A.

Tvrzení 1. Buď $(A,*)$ pologrupa, $(B,*)$ podpologrupa v $(A,*)$ a $(C,*)$ podpologrupa v $(B,*)$. Pak $(C,*)$ je podpologrupa $(A,*)$.

2. Buď $(A,*)$ pologrupa, $(B,*)$, $(C,*)$ podpologrupy v $(A,*)$. Pak $(B \cap C,*)$ je podpologrupa v $(A,*)$.

Tvrzení Podmnožiny $m\mathbb{Z} \subseteq \mathbb{Z}$ jsou podgrupy v grupě $(\mathbb{Z},+,0,-)$ a jiné podgrupy tam nejsou.

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