Pologrupy, monoidy, grupy

Jan Paseka

Masarykova univerzita Brno

Abstrakt

V této kapitole se budeme zabývat jistými speciálními typy zobrazení, které se nazývají operace.

Abstrakt

V této kapitole se budeme zabývat jistými speciálními typy zobrazení, které se nazývají operace.
Pojem operace vznikl zobecněním pojmů běžně známých ze střední školy, jako jsou například násobení přirozených čísel nebo odečítání celých čísel, atd.

Abstrakt

V této kapitole se budeme zabývat jistými speciálními typy zobrazení, které se nazývají operace.
Pojem operace vznikl zobecněním pojmů běžně známých ze střední školy, jako jsou například násobení přirozených čísel nebo odečítání celých čísel, atd.
Vidíme, že v těchto případech je vždy libovolné uspořádané dvojici čísel z jisté množiny přiřazeno jediné, přesně určené číslo z téže množiny.

Obsah přednášky

- Operace, grupoid.
- n–ární operace.
- Asociativní operace, pologrupa.
- Komutativní zákon.

Obsah přednášky

- Operace, grupoid.
- n–ární operace.
- Asociativní operace, pologrupa.
- Komutativní zákon.
- Monoid.
- Invertibilní a inverzní prvek.
- Grupa.

Grupoid

Definice. Nechť G je neprázdná množina. Pak libovolné zobrazení $G \times G \longrightarrow G$ se nazývá **operace na množině** G.

Grupoid

Definice. Nechť G je neprázdná množina. Pak libovolné zobrazení $G \times G \longrightarrow G$ se nazývá **operace na množině** G.

Je – li při tomto zobrazení uspořádané dvojici $(a, b) \in G$ přiřazen prvek $c \in G$, pak budeme obvykle psát $\boxed{a \cdot b = c}$ a hovořit o operaci $\cdot$ (čti "tečka") .

Množina G spolu s operací $\cdot$ se nazývá **grupoid** a označuje se symbolem $\boxed{(G, \cdot)}$.

Grupoid

Definice. Nechť G je neprázdná množina. Pak libovolné zobrazení $G \times G \longrightarrow G$ se nazývá **operace na množině** G.

Je – li při tomto zobrazení uspořádané dvojici $(a, b) \in G$ přiřazen prvek $c \in G$, pak budeme obvykle psát $\boxed{a \cdot b = c}$ a hovořit o operaci $\cdot$ (čti "tečka") .

Množina G spolu s operací $\cdot$ se nazývá **grupoid** a označuje se symbolem $\boxed{(G, \cdot)}$.

Označení I

Poznámka.

1. Pro označování operace na množině G se ukazuje jako nepraktické používat písmena a symboliku zavedenou v kapitole o zobrazeních. Vhodnější je používat speciálních symbolů. Nejčastěji to budou:

Označení I

Poznámka.

1. Pro označování operace na množině G se ukazuje jako nepraktické používat písmena a symboliku zavedenou v kapitole o zobrazeních. Vhodnější je používat speciálních symbolů. Nejčastěji to budou:
   - symbol $\cdot$ (tzv. multiplikativní symbolika), který budeme číst ”krát” a budeme hovořit o operaci ”násobení”. Je–li $a \cdot b = c$, pak prvek c budeme nazývat součinem prvků a, b (v tomto pořadí).

Označení II

– symbol $+$ (tzv. aditivní symbolika), který budme číst ”plus” a budeme hovořit o operaci ”sečítání”. Je–li $a + b = c$, pak prvek c budeme nazývat součtem prvků a, b (v tomto pořadí).

Označení II

– symbol $+$ (tzv. aditivní symbolika), který budme číst ”plus” a budeme hovořit o operaci ”sečítání”. Je–li $a + b = c$, pak prvek c budeme nazývat součtem prvků a, b (v tomto pořadí).

Výše zavedené symboly $\cdot$ nebo $+$ samozřejmě nemají nic společného s násobením nebo sčítáním čísel. Pro označování operací na množině budeme podle potřeby používat i jiné symboly, například $\circ$, $*$ atd.

Nosná množina grupoidu

2. Z předchozí definice plyne, že grupoid $(G, \cdot)$ je uspořádaná dvojice, sestávající z množiny G (která se též nazývá **nosná množina grupoidu**) a z operace $\cdot$ na množině G.

Nosná množina grupoidu

2. Z předchozí definice plyne, že grupoid $(G, \cdot)$ je uspořádaná dvojice, sestávající z množiny G (která se též nazývá **nosná množina grupoidu**) a z operace $\cdot$ na množině G.

   Rovnost dvou grupoidů znamená tedy rovnost nosných množin a současně rovnost příslušných operací.

n – ární operace I

"n – ární operace" na množině G, pro libovolné přirozené n, což je libovolné zobrazení $G \times G \times \cdots \times G$ (n – krát) $\longrightarrow G$.

n – ární operace I

"n – ární operace" na množině G, pro libovolné přirozené n, což je libovolné zobrazení $G \times G \times \cdots \times G$ (n – krát) $\longrightarrow G$.

Je to předpis, který každé uspořádané n – tici prvků z G přiřazuje jediný prvek z G.

n – ární operace I

"n – ární operace" na množině G, pro libovolné přirozené n, což je libovolné zobrazení $G \times G \times \cdots \times G$ (n – krát) $\longrightarrow G$.

Je to předpis, který každé uspořádané n – tici prvků z G přiřazuje jediný prvek z G.

Příkladem n – ární operace na množině reálných čísel $\mathbf{R}$ je třeba operace max $(x_1, x_2, \ldots, x_n)$, která každé uspořádané n – tici reálných čísel přiřazuje to číslo, které je z nich maximální.

n – ární operace II

Pro $n = 1$, resp. $n = 2$, resp. $n = 3$ se pak užívá názvů unární operace, resp. binární operace, resp. ternární operace.

n – ární operace II

Pro $n = 1$, resp. $n = 2$, resp. $n = 3$ se pak užívá názvů unární operace, resp. binární operace, resp. ternární operace.

Unární operace na G není nic jiného, než libovolné zobrazení $G \longrightarrow G$.

n – ární operace II

Pro $n = 1$, resp. $n = 2$, resp. $n = 3$ se pak užívá názvů unární operace, resp. binární operace, resp. ternární operace.

Unární operace na G není nic jiného, než libovolné zobrazení $G \longrightarrow G$.

Binární operace je pak operací v našem slova smyslu, definovanou výše.

Příklady I

1. Uvažme množinu $\mathbb{Z}$ všech celých čísel. Pak obyčejné násobení čísel $\cdot$ je zřejmě operací na množině $\mathbb{Z}$. Tedy $(\mathbb{Z}, \cdot)$ je grupoid.

Příklady I

1. Uvažme množinu $\mathbb{Z}$ všech celých čísel. Pak obyčejné násobení čísel $\cdot$ je zřejmě operací na množině $\mathbb{Z}$. Tedy $(\mathbb{Z}, \cdot)$ je grupoid.

   Podobně dostáváme grupoidy $(\mathbb{Z}, +)$, resp. $(\mathbb{Z}, -)$, kde $+$, resp. $-$ značí obyčejné sčítání, resp. obyčejné odečítání celých čísel.

Příklady I

1. Uvažme množinu $\mathbb{Z}$ všech celých čísel. Pak obyčejné násobení čísel $\cdot$ je zřejmě operací na množině $\mathbb{Z}$. Tedy $(\mathbb{Z}, \cdot)$ je grupoid.

   Podobně dostáváme grupoidy $(\mathbb{Z}, +)$, resp. $(\mathbb{Z}, -)$, kde $+$, resp. $-$ značí obyčejné sčítání, resp. obyčejné odečítání celých čísel.

   Je jasné, že se jedná o různé grupoidy, i když nosná množina je ve všech třech případech stejná.

Příklady II

2. Vezmeme–li množinu $\mathbb{N}$ všech přirozených čísel, pak obyčejné odečítání čísel není operací na $\mathbb{N}$, protože například pro přirozená čísla $2, 3$ je $2 - 3 \notin \mathbb{N}$, tzn. nejedná se o zobrazení $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.

Příklady II

2. Vezmeme–li množinu $\mathbb{N}$ všech přirozených čísel, pak obyčejné odečítání čísel není operací na $\mathbb{N}$, protože například pro přirozená čísla $2, 3$ je $2 - 3 \notin \mathbb{N}$, tzn. nejedná se o zobrazení $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.

   Dále například obyčejné dělení čísel není operací na množině $\mathbb{R}$ všech reálných čísel.

Příklady III

3. Nechť A je libovolná množina. Pak sjednocení, průnik a rozdíl dvou podmnožin množiny A je opět (jednoznačně určená) podmnožina v A.

Příklady III

3. Nechť A je libovolná množina. Pak sjednocení, průnik a rozdíl dvou podmnožin množiny A je opět (jednoznačně určená) podmnožina v A.

   Tedy sjednocení, průnik a rozdíl množin jsou operace na množině 2^A (tj. na systému všech podmnožin množiny A).

Příklady III

3. Nechť A je libovolná množina. Pak sjednocení, průnik a rozdíl dvou podmnožin množiny A je opět (jednoznačně určená) podmnožina v A.

   Tedy sjednocení, průnik a rozdíl množin jsou operace na množině 2^A (tj. na systému všech podmnožin množiny A).

   Dostáváme tak grupoidy $(2^A, \cup)$, resp. $(2^A, \cap)$, resp. $(2^A, -)$.

Příklady IV

4. Nechť A je libovolná neprázdná množina. Symbolem A^A, jak víme, označujeme systém všech zobrazení množiny A do množiny A.

Příklady IV

4. Nechť A je libovolná neprázdná množina. Symbolem A^A, jak víme, označujeme systém všech zobrazení množiny A do množiny A.

   Pro $f, g \in A^A$ je zřejmě složené zobrazení $g \circ f$ opět zobrazením $A \longrightarrow A$, tzn. jinak řečeno $g \circ f \in A^A$.

Příklady IV

4. Nechť A je libovolná neprázdná množina. Symbolem A^A, jak víme, označujeme systém všech zobrazení množiny A do množiny A.

   Pro $f, g \in A^A$ je zřejmě složené zobrazení $g \circ f$ opět zobrazením $A \longrightarrow A$, tzn. jinak řečeno $g \circ f \in A^A$.

   Skládání zobrazení je tedy operací na množině A^A a $(A^A, \circ)$ je pak grupoid.

Zadávání operace

Operace na množině G je zobrazení $G \times G \longrightarrow G$.

Zadávání operace

Operace na množině G je zobrazení $G \times G \longrightarrow G$.

Je to tedy předpis, který každé uspořádané dvojici prvků z G přiřadí jediný prvek z G.

Zadávání operace

Operace na množině G je zobrazení $G \times G \longrightarrow G$.

Je to tedy předpis, který každé uspořádané dvojici prvků z G přiřadí jediný prvek z G.

Pokud je však množina G konečná, pak je výhodné zadávat operaci na G pomocí tabulky.

Příklad V

5. Na množině $G = \{a, b, c, d\}$ definujeme operaci $\cdot$ tabulkou:

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

Příklad V

5. Na množině $G = \{a, b, c, d\}$ definujeme operaci $\cdot$ tabulkou:

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

Potom $(G, \cdot)$ je grupoid, přičemž například platí: $a \cdot d = c$, $d \cdot a = a$ atd.

Vlastnosti grupoidů I

Nechť $(G, \cdot)$ je grupoid.

Vlastnosti grupoidů I

Nechť $(G, \cdot)$ je grupoid.

Je-li pro každá $a, b, c \in G$ splněno

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

pak o operaci $\cdot$ říkáme, že je to **asociativní** operace, a o grupoidu $(G, \cdot)$ mluvíme jako o asociativním grupoidu, anebo častěji říkáme, že $(G, \cdot)$ je **pologrupa**.

Vlastnosti grupoidů II

Nechť $(G, \cdot)$ je grupoid.

Vlastnosti grupoidů II

Nechť $(G, \cdot)$ je grupoid.

Je-li pro každá $a, b \in G$ splněno

$$a \cdot b = b \cdot a,$$

pak o operaci $\cdot$ říkáme, že je to **komutativní** operace, a o grupoidu $(G, \cdot)$ mluvíme jako o komutativním grupoidu.

Vlastnosti grupoidů III

Tvrzení. Buď $(G, \cdot)$ pologrupa. Pak pro libovolné přirozené číslo n a pro libovolná $a_1, a_2, \ldots, a_n \in G$ výsledek součinu prvků $a_1, a_2, \ldots, a_n$ v dané pologrupě v uvedeném pořadí nezávisí na jejich uzávorkování.

Vlastnosti grupoidů III

Tvrzení. Buď $(G, \cdot)$ pologrupa. Pak pro libovolné přirozené číslo n a pro libovolná $a_1, a_2, \ldots, a_n \in G$ výsledek součinu prvků $a_1, a_2, \ldots, a_n$ v dané pologrupě v uvedeném pořadí nezávisí na jejich uzávorkování.

Poznámka. Proto pak takový součin zapisujeme ve tvaru $a_1 \cdot a_2 \cdot \ldots \cdot a_n$.

Vlastnosti grupoidů IV

Tvrzení. Buď $(G, \cdot)$ komutativní pologrupa. Pak pro libovolné přirozené číslo n a pro libovolná $a_1, a_2, \ldots, a_n \in G$ výsledek součinu prvků $a_1, a_2, \ldots, a_n$ nezávisí na jejich pořadí ani uzávorkování.

Vlastnosti grupoidů IV

Tvrzení. Buď $(G, \cdot)$ komutativní pologrupa. Pak pro libovolné přirozené číslo n a pro libovolná $a_1, a_2, \ldots, a_n \in G$ výsledek součinu prvků $a_1, a_2, \ldots, a_n$ nezávisí na jejich pořadí ani uzávorkování.

Nechť $(G, \cdot)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** nebo též **jednotkový prvek** grupoidu $(G, \cdot)$, je-li pro každý prvek $a \in G$ splněno

$$e \cdot a = a = a \cdot e.$$

Příklady VI

a) Grupoidy $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, +)$, $(2^A, \cup)$, $(2^A, \cap)$ jsou asociativní i komutativní, jednotkový prvek je po řadě 1, 0, $\emptyset$ a A.

Příklady VI

a) Grupoidy $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, +)$, $(2^A, \cup)$, $(2^A, \cap)$ jsou asociativní i komutativní, jednotkový prvek je po řadě 1, 0, $\emptyset$ a A.

b) Grupoid $(\mathbb{Z}, -)$ a grupoid $(G, \cdot)$ z příkladu V není asociativní a není komutativní. První grupoid nemá jednotkový prvek, u druhého je jednotkovým prvkem prvek b.

Příklady VI

c) Grupoid $(2^A, -)$ je asociativní i komutativní v případě, že $A = \emptyset$; je–li $A \neq \emptyset$, pak $(2^A, -)$ není asociativní ani komutativní. Grupoid nemá jednotkový prvek.

Příklady VI

c) Grupoid $(2^A, -)$ je asociativní i komutativní v případě, že $A = \emptyset$; je–li $A \neq \emptyset$, pak $(2^A, -)$ není asociativní ani komutativní. Grupoid nemá jednotkový prvek.

d) Grupoid $(A^A, \circ)$ je vždy asociativní; komutativní je tento grupoid pouze v případě, že množina A je jednoprvková. Jednotkový prvek je identické zobrazení.

Jednotkový prvek, monoid

Tvrzení. V libovolném grupoidu $(G, \cdot)$ existuje nejvýše jeden jednotkový prvek.

Jednotkový prvek, monoid

Tvrzení. V libovolném grupoidu $(G, \cdot)$ existuje nejvýše jeden jednotkový prvek.

Z uvedeného tvrzení plyne, že má-li grupoid jednotkový prvek, je tento prvek jednoznačně určen. Proto se zpravidla značí symbolem 1.

Jednotkový prvek, monoid

Tvrzení. V libovolném grupoidu $(G, \cdot)$ existuje nejvýše jeden jednotkový prvek.

Z uvedeného tvrzení plyne, že má-li grupoid jednotkový prvek, je tento prvek jednoznačně určen. Proto se zpravidla značí symbolem 1.

Je-li $(G, \cdot)$ pologrupa, která obsahuje jednotkový prvek 1, říkáme, že $(G, \cdot)$ je **monoid**.

Invertibilní a inverzní prvek

Nechť $(G, \cdot)$ je grupoid s jednotkovým prvkem $\mathtt{1}$. Jestliže pro některý prvek $a \in G$ existuje prvek $b \in G$ takový, že platí

$$a \cdot b = \mathtt{1} = b \cdot a,$$

pak prvek a se nazývá **invertibilní prvek** grupoidu $(G, \cdot)$ a prvek b se nazývá **inverzní prvek** k prvku a v tomto grupoidu.

Invertibilní a inverzní prvek

Nechť $(G, \cdot)$ je grupoid s jednotkovým prvkem 1. Jestliže pro některý prvek $a \in G$ existuje prvek $b \in G$ takový, že platí

$$a \cdot b = 1 = b \cdot a,$$

pak prvek a se nazývá **invertibilní prvek** grupoidu $(G, \cdot)$ a prvek b se nazývá **inverzní prvek** k prvku a v tomto grupoidu.

Tvrzení. V libovolném monoidu $(G, \cdot)$ existuje ke každému prvku $a \in G$ nejvýše jeden inverzní prvek.

Počítání s invertibilními prvky

Existuje-li v monoidu $(G, \cdot)$ k prvku $a \in G$ inverzní prvek, je tento prvek jediný a zpravidla se značí symbolem a^{-1}.

Počítání s invertibilními prvky

Existuje-li v monoidu $(G, \cdot)$ k prvku $a \in G$ inverzní prvek, je tento prvek jediný a zpravidla se značí symbolem a^{-1}.

Tvrzení. Nechť $(G, \cdot)$ je monoid a nechť 1 je jeho jednotkový prvek. Nechť n je přirozené číslo a nechť $a, a_1, a_2, \ldots, a_n \in G$ jsou libovolné invertibilní prvky monoidu $(G, \cdot)$. Pak 1, a^{-1} a $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ jsou rovněž invertibilní prvky a platí rovnosti

$$1^{-1} = 1,$$

$$(a^{-1})^{-1} = a,$$

$$(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_2^{-1} \cdot a_1^{-1}.$$

Grupa

Monoid $(G, \cdot)$, v němž ke každému prvku existuje prvek inverzní, to znamená monoid, jehož všechny prvky jsou invertibilní, se nazývá **grupa**.

Grupa

Monoid $(G, \cdot)$, v němž ke každému prvku existuje prvek inverzní, to znamená monoid, jehož všechny prvky jsou invertibilní, se nazývá **grupa**.

Příklady. Dvojice $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}-\{0\}, \cdot)$, $(\mathbb{R}-\{0\}, \cdot)$, $(\mathbb{C}-\{0\}, \cdot)$ jsou komutativní grupy.

Příklady grup I

Buď A libovolná množina a buď $\mathcal{P}(A)$ potenční množina množiny A.

Příklady grup I

Buď A libovolná množina a buď $\mathcal{P}(A)$ potenční množina množiny A.

Definujeme na množině $\mathcal{P}(A)$ binární operaci $\div$ **symetrické diference** následujícím předpisem. Pro libovolné dvě podmnožiny $B, C \subseteq A$ klademe

$$B \div C = (B \cup C) - (B \cap C) = (B - C) \cup (C - B).$$

Příklady grup I

Buď A libovolná množina a buď $\mathcal{P}(A)$ potenční množina množiny A.

Definujeme na množině $\mathcal{P}(A)$ binární operaci $\div$ **symetrické diference** následujícím předpisem. Pro libovolné dvě podmnožiny $B, C \subseteq A$ klademe

$$B \div C = (B \cup C) - (B \cap C) = (B - C) \cup (C - B).$$

Tato operace je asociativní na $\mathcal{P}(A)$, $(\mathcal{P}(A), \div)$ je komutativní grupa, neboť jednotkovým prvkem je zde prázdná podmnožina $\emptyset$ a každá podmnožina $B \subseteq A$ je zde inverzním prvkem sama k sobě.

Příklady grup II

Vezměme opět libovolnou množinu X a uvažujme dále libovolné bijekce $f : X \to X$ (permutace množiny X).

Příklady grup II

Vezměme opět libovolnou množinu X a uvažujme dále libovolné bijekce $f : X \to X$ (permutace množiny X).

Skládání zobrazení $\circ$ je operací též na množině $S(X)$ všech permutací, takže dvojice $\boxed{(S(X), \circ)}$ je monoid, a je to dokonce grupa, neboť pro každou permutaci $f : X \to X$ je inverzní zobrazení $f^{-1} : X \to X$ permutací, která je k ní inverzním prvkem.

Příklady grup II

Vezměme opět libovolnou množinu X a uvažujme dále libovolné bijekce $f : X \to X$ (permutace množiny X).

Skládání zobrazení $\circ$ je operací též na množině $S(X)$ všech permutací, takže dvojice $\boxed{(S(X), \circ)}$ je monoid, a je to dokonce grupa, neboť pro každou permutaci $f : X \to X$ je inverzní zobrazení $f^{-1} : X \to X$ permutací, která je k ní inverzním prvkem.
Uvedená grupa se nazývá **grupa permutací** množiny X. Obecně není komutativní.

Grupa invertibilních prvků monoidu

Důsledek. Nechť $(G, \cdot)$ je monoid a nechť $H \subseteq G$ je množina všech invertibilních prvků monoidu $(G, \cdot)$. Pak množina H je uzavřená vzhledem k operaci $\cdot$, čili tato operace je operací i na množině H, a přitom dvojice $(H, \cdot)$ je grupa.

Grupa S_3

Prvky množiny $\mathcal{S}_3$, t. j. permutace množiny $\{1, 2, 3\}$, si můžeme představit jako symetrie rovnostranného trojúhelníka s vrcholy označenými čísly 1, 2, 3.

Označme si identickou permutaci této množiny jako ι, otočení kolem těžiště trojúhelníka proti směru resp. ve směru hodinových ručiček o uhel $\pi/3$ jako ϱ resp. ϱ^{-1}, a osovou souměrnost podle osy procházející i-tým vrcholem a středem protilehlé strany jako σ_i, pro $i = 1,\ 2,\ 3$.

Grupa S_3

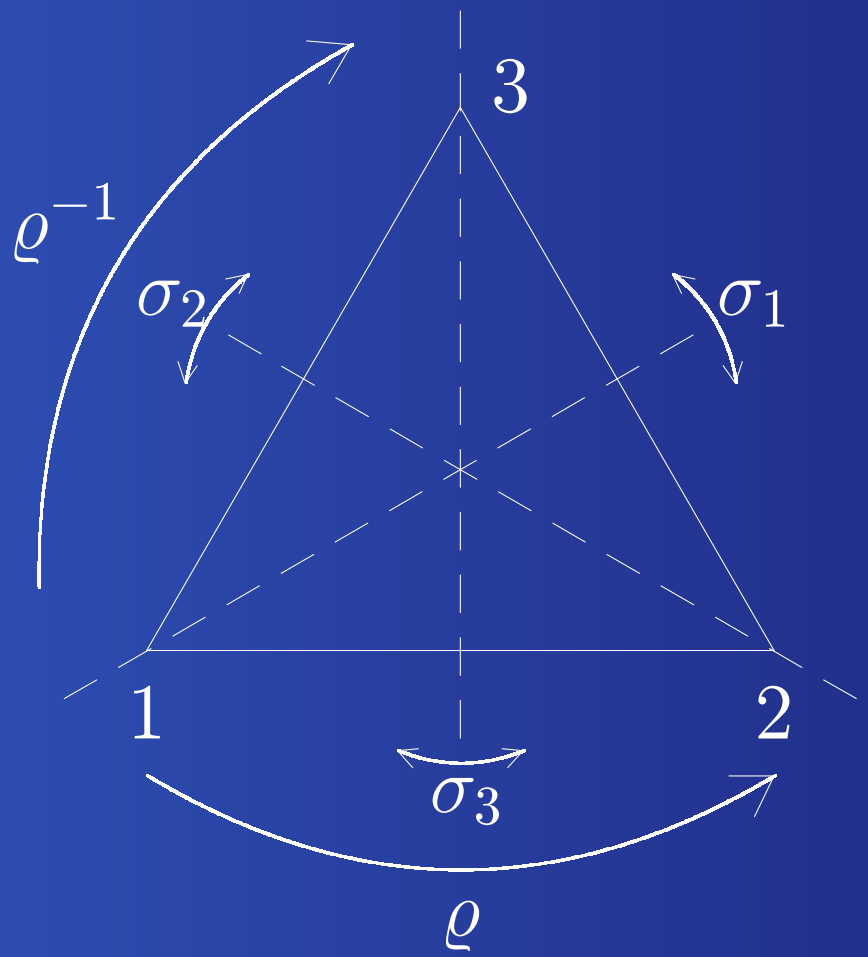
Množina permutací $\mathcal{S}_3$ se bude skládat z permutací

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$\varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Grupa S_3



Grupa S_3

Multiplikativní tabulka binární operace $\circ$ na množině $\mathcal{S}_3$ má následující tvar:

$\circ$	ι	ϱ	ϱ^{-1}	σ_1	σ_2	σ_3
ι	ι	ϱ	ϱ^{-1}	σ_1	σ_2	σ_3
ϱ	ϱ	ϱ^{-1}	ι	σ_3	σ_1	σ_2
ϱ^{-1}	ϱ^{-1}	ι	ϱ	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	ι	ϱ	ϱ^{-1}
σ_2	σ_2	σ_3	σ_1	ϱ^{-1}	ι	ϱ
σ_3	σ_3	σ_1	σ_2	ϱ	ϱ^{-1}	ι