Cyklické a permutační grupy

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Podgrupy konečných cyklických grup

Věta 11

Nechť G je cyklická grupa s n prvky, která je generovaná a a $b = a^s \in G$.

- *b generuje cyklickou podgrupu $H \leq G$ obsahující n/d prvků, kde d je $gcd(n, s)$.*
- *$\langle a^s \rangle = \langle a^t \rangle$ právě když $gcd(s, n) = gcd(t, n)$.*

Důkaz

Dle věty 6: b generuje cyklickou podgrupu H grupy G.
Chceme ukázat, že $\underline{H \text{ má } n/d \text{ prvků}}$.
Dle věty 10: H má tolik prvků, jako nejmenší kladná mocnina m čísla b, která nám dá neutrální prvek.
$b = a^s$ a $b^m = e$ právě, když $(a^s)^m = e$, tedy, když n dělí ms.
Hledáme nejmenší kladné číslo m takové, že n dělí ms.

Podgrupy konečných cyklických grup

Důkaz (Pokračování)

Nechť $d = gcd(n, s)$. *Pak existují* $u, v \in \mathbb{Z}$ *taková, že*
$d = un + vs$.
Protože d *dělí* n *i* s, *můžeme psát*
$1 = u(n/d) + v(s/d)$ *(*(n/d) *i* (s/d) *jsou celá čísla)*
Zřejmě n/d *a* s/d *jsou nesoudělná čísla.*
Hledáme kladné m *takové, že*
$\frac{ms}{n} = \frac{m(s/d)}{(n/d)}$ *je celé číslo.*
Z toho, že pokud jsou r *a* s *nesoudělná a pokud* r *dělí* sm, *pak* r *dělí* m *dostáváme, že* n/d *musí dělit* m, *takže nejmenší kladné takové* m *je* n/d. *Řád* H *je tedy* n/d.

Podgrupy konečných cyklických grup

Důkaz (Pokračování)

$\langle a^s \rangle = \langle a^t \rangle$, právě když $gcd(s,n) = gcd(t,n)$

Všechny cyklické grupy řádu n jsou isomorfní s $\mathbb{Z}_n$.
Pokud je d dělitelem n, pak cyklická podgrupa $\langle d \rangle$ grupy $\mathbb{Z}_n$ má n/d prvků a obsahuje všechna přirozená čísla m menší než n taková, že $gcd(m,n) = d$.
Takže existuje jenom jedna podgrupa $\mathbb{Z}_n$ řádu n/d.
Pokud je a generátor cyklické grupy G, pak $\langle a^s \rangle = \langle a^t \rangle$, právě když $gcd(s,n) = gcd(t,n)$.

Podgrupy konečných cyklických grup

Příklad 27

$\mathbb{Z}_{12}$ *má generátor* 1. *Jak vypadají následující podgrupy a kolik mají prvků?*

1. $\langle 3 \rangle$
2. $\langle 8 \rangle$
3. $\langle 5 \rangle$

Podgrupy konečných cyklických grup

Příklad

$\mathbb{Z}_{12}$ má generátor 1. Jak vypadají následující podgrupy a kolik mají prvků?

1. $\langle 3 \rangle = \{0, 3, 6, 9\}$
   - $gcd(3, 12) = 3$
   - 3 generuje podgrupu o $\frac{12}{3} = 4$ prvcích
2. $\langle 8 \rangle = \{0, 4, 8\}$
   - $gcd(8, 12) = 4$
   - 4 generuje podgrupu o $\frac{12}{4} = 3$ prvcích
3. $\langle 5 \rangle = \mathbb{Z}_{12}$
   - $gcd(5, 12) = 1$
   - 5 generuje podgrupu o $\frac{12}{1} = 12$ prvcích, tedy celou grupu

Podgrupy konečných cyklických grup

Důsledek 3

Pokud je generátor cyklické grupy G řádu n, pak ostatní generátory G jsou prvky tvaru a^r, kde r je nesoudělné s n.

Příklad 28

Pro grupu $\mathbb{Z}_{18}$ najděte všechny podgrupy a zobrazte jejich diagram.

Podgrupy konečných cyklických grup

Příklad

Pro grupu $\mathbb{Z}_{18}$ najděte všechny podgrupy a zobrazte jejich diagram.

- Grupa je cyklická, všechny podgrupy jsou cyklické.
- Dle důsledku 3 jsou generátory prvky: 1, 5, 7, 11, 13 a 17 (generují celou grupu)
- $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
  grupa řádu 9, její generátory jsou prvky ve tvaru $h2$, kde h jsou nesoudělná s 9 ($h = 1, 2, 4, 5, 7, 9$, takže $h2 = 2, 4, 8, 10, 14, 16$).
- Prvek 6 z $\langle 2 \rangle$ generuje $\{0, 6, 12\}$ (stejně jako 12. **Proč?**)
- $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$ (stejnou grupu generuje i 15. **Proč?**)
- $\langle 9 \rangle = \{0, 9\}$

$$
\begin{tikzcd}[column sep=small]
 & \langle \mathbf{1} \rangle = \mathbb{Z}_{18} \arrow[dl, no head] \arrow[dr, no head] & & \\
\langle \mathbf{2} \rangle \arrow[dr, no head] & & \langle \mathbf{3} \rangle \arrow[dl, no head] \arrow[dr, no head] & \\
 & \langle \mathbf{6} \rangle \arrow[dr, no head] & & \langle \mathbf{9} \rangle \arrow[dl, no head] \\
 & & \langle \mathbf{0} \rangle &
\end{tikzcd}
$$

Generující množiny

- G je grupa, $a, b \in G$
- Nejmenší cyklická podgrupa, která obsahuje a i b, zřejmě (dle věty 6) obsahuje i a^m, b^n pro všechna $a, b \in \mathbb{Z}$
- Navíc musí obsahovat všechny konečné součiny takových mocnin a a b
  Např. $a^2 b^1 a^{-5}$
- Pokud není G abelovská, nemůžeme napsat nejprve mocniny a a pak mocniny b
- Všechny takové součiny mocnin a a b tvoří podgrupu grupy G, což musí být nejmenší podgrupa obsahující a a b
- Prvky a a b nazýváme **generátory této podgrupy**.
- Pokud je podgrupa celá grupa G, říkáme, že $\{a, b\}$ **generuje** G.
- Generátory mohou být množiny obsahující více než 2 prvky

Generující množiny

Příklad 29

Kleinova 4-grupa $\langle V = \{e, a, b, c\}, \circ\rangle$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

je generovaná $\{a, b\}$, *protože* $ab = c$.

Jakými dalšími množinami je generovaná?

Generující množiny

Příklad

Kleinova 4-grupa $\langle V = \{e, a, b, c\}, \circ\rangle$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

je generovaná $\{a, b\}$, *protože* $ab = c$.
Jakými dalšími množinami je generovaná?

- Je generovaná $\{a, b\}$, $\{a, c\}$, $\{b, c\}$
- Pokud je grupa G generovaná podmnožinou S, pak každá podmnožina, která obsahuje S generuje G
  $\{a, b, c\}$, $\{a, b, e\}$, $\{a, c, e\}$, $\{b, c, e\}$, $\{a, b, c, e\}$

Generující množiny

Příklad 30

Grupa $\mathbb{Z}_6$ *je generovaná* $\{1\}$ *a* $\{5\}$.
Protože $2 + 3 = 5$, *pak podgrupa obsahující* 2 *a* 3 *musí také obsahovat* 5. *Odtud vidíme, že je rovna* $\mathbb{Z}_6$. $\{2, 3\}$ *tedy generuje* $\mathbb{Z}_6$.
Jakými dalšími množinami je generovaná?

Generující množiny

Příklad

Grupa $\mathbb{Z}_6$ *je generovaná* $\{1\}$ *a* $\{5\}$.
Protože $2 + 3 = 5$, *pak podgrupa obsahující* 2 *a* 3 *musí také obsahovat* 5. *Odtud vidíme, že je rovna* $\mathbb{Z}_6$. $\{2, 3\}$ *tedy generuje* $\mathbb{Z}_6$.
Jakými dalšími množinami je generovaná?

- Je také generovaná libovolnou podmnožinou obsahující 1 nebo 5 (např. $\{1, 2\}$)
- Je také generovaná libovolnou podmnožinou obsahující 2 a 3 (např. $\{2, 3, 4\}$)
- $\{3, 4\}$ a podmnožiny obsahující 3 a 4 (např. $\{2, 3, 4\}$)
- Není však generovaná $\{2, 4\}$

Průnik množin

Definice

Nechť $\{S_i | i \in I\}$ *je kolekce množin (*I *je množina indexů).* **Průnik množin** S_i *(značíme* $\bigcap_{i \in I} S_i$*) je množina všech prvků, které jsou ve všech množinách* S_i*:*
$\bigcap_{i \in I} S_i = \{x | x \in S_i, \forall i \in I\}$*.*
Pokud je I *konečná (*$I = \{1, 2, \dots, n\}$*), pak zapisujeme*
$S_1 \cap S_2 \cap \dots \cap S_n$*.*

Průnik množin

Věta 12

Průnik podgrup H_i grupy G pro $i \in I$ je opět podgrupa G.

Důkaz

Uzavřenost na operaci:

Nechť $a \in \bigcap_{i \in I} H_i$ a $b \in \bigcap_{i \in I} H_i$, takže $a \in H_i$ a $b \in H_i$ pro všechna $i \in I$. Pak $ab \in H_i$ pro všechna $i \in I$, protože H_i je grupa. Takže $ab \in \bigcap_{i \in I} H_i$.

Existence neutrálního prvku:

$e \in H_i$ pro všechna $i \in I$, protože H_i je grupa. Takže $e \in \bigcap_{i \in I} H_i$.

Inverzní prvky:

Pro $a \in \bigcap_{i \in I} H_i$ máme $a \in H_i$ pro všechna $i \in I$. Protože H_i je grupa $a^{-1} \in H_i$. Tedy $a^{-1} \in \bigcap_{i \in I} H_i$.

Generátory grupy

Definice

Nechť G *je grupa a* $a_i \in G$ *pro* $i \in I$. *Nejmenší podgrupa* G *obsahující* $\{a_i | i \in I\}$ *je* **podgrupa generovaná** $\{a_i | i \in I\}$. *Pokud je tato podgrupa celá grupa* G, *pak* $\{a_i | i \in I\}$ **generuje** G *a* a_i *jsou* **generátory** *grupy* G. *Pokud existuje konečná množina* $\{a_i | i \in I\}$, *která generuje* G, *pak* G *je* **konečně generovaná**.

Tato definice je konzistentní s dříve zmíněnou definicí generátoru cyklické grupy.

Generátory grupy

Věta 13

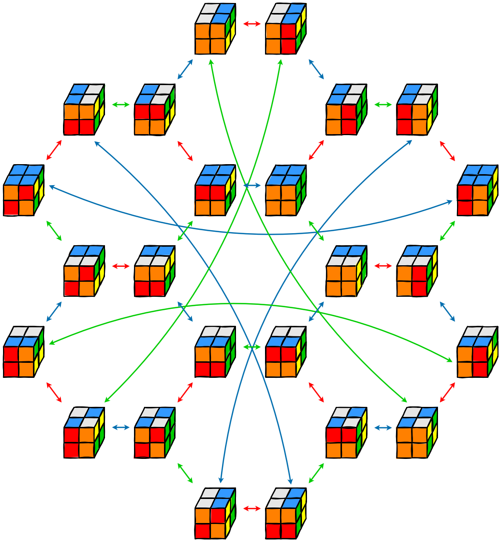
Pokud G je grupa a $a_i \in G$ pro $i \in I$, pak podgrupa H grupy G generovaná $\{a_i | i \in I\}$ má právě ty prvky grupy G, které jsou konečné součiny celočíselných mocnin a_i (mocniny stejného a_i se mohou vyskytovat víckrát).

Důkaz

Nechť K označuje množinu všech konečných součinů mocnin a_i. Pak $K \subseteq H$.
Potřebujeme jen ověřit, že K je podgrupa (H je nejmenší podgrupa obsahující a_i):
Součin prvků z K je opět v K. Protože $(a_i)^0 = e$, máme $e \in K$. Pro každý prvek $k \in K$, pokud vytvoříme součin, kde bude pořadí a_i obrácené a exponenty budou mít opačná znaménka, dostaneme k^{-1}, které je v K.
Např. $(a_1)^3(a_2)^{-2}$ a $(a_2)^2(a_1)^{-3}$

Caleyho grafy

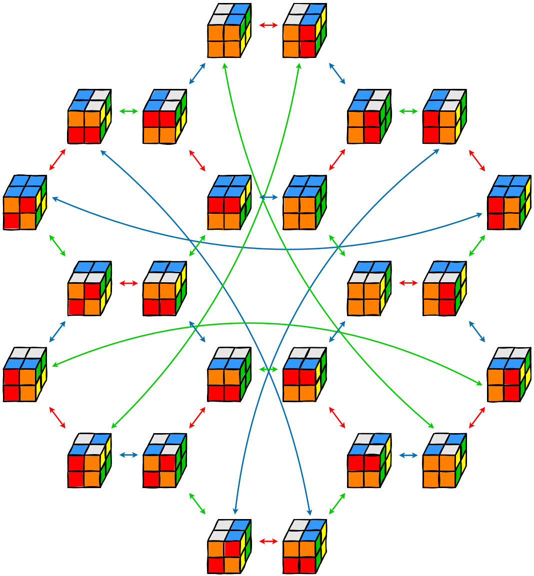
- **Caleyho graf** – vizualizace konečné grupy pomocí generátorů, navrženy Cayleym
- Pro každou generující množinu S konečné grupy G – orientovaný graf reprezentující tuto grupu pomocí generátorů
- Graf se skládá z konečného počtu bodů (vrcholů), pro každý prvek grupy jeden
- Orientované hrany mezi vrcholy – každý generátor v S je označen jedním typem hran (budeme používat různé barvy nebo typy čar)



Vlastnosti Caleyho grafu

Graf je spojitý(můžeme najít cestu mezi každými dvěma uzly).

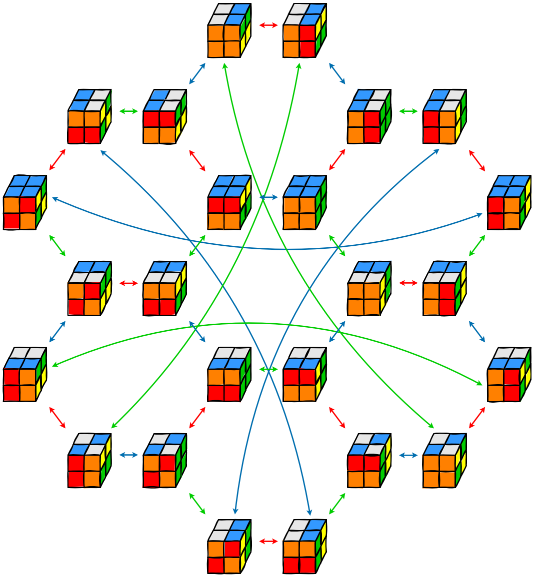
<u>Důvod</u>: Každá rovnice $gx = h$ má řešení v grupě.



Vlastnosti Caleyho grafu

Nejvýše jedna hrana jde z jednoho vrcholu do druhého.

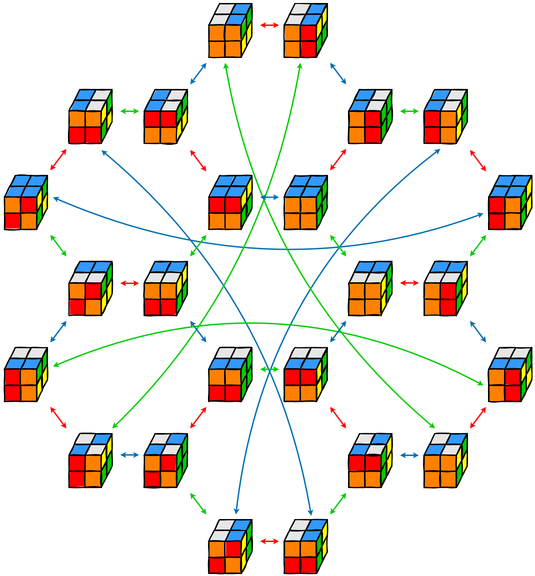
Důvod: Každá rovnice $gx = h$ je unikátní.



Vlastnosti Caleyho grafu

Každý uzel má právě jednu hranu každého typu, která v něm začíná, a jednu každého typu, která v něm končí.

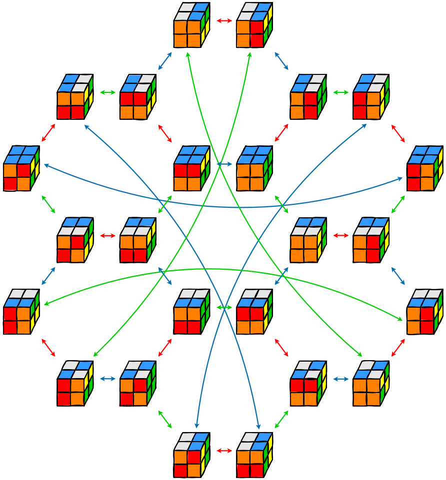
Důvod: pro $g \in G$ a každý generátor b můžeme spočítat gb a $(gb^{-1})b = g$.



Vlastnosti Caleyho grafu

Pokud dvě různé posloupnosti typů hran začínající v g vedou do stejného uzlu h, pak tytéž posloupnosti začínající v libovolném uzlu u povedou do stejného uzlu v.

<u>Důvod</u>: Pokud $gq = h$ a $gr = h$, pak $uq = ug^{-1}h = ur$.



Příklad 31

Najděte dvě různé cesty z  *do* .

Použijte stejné cesty z .

Možná otočení Rubikovy kostky $(3 \times 3 \times 3)$ tvoří grupu s $43\ 252\ 003\ 274\ 489\ 856\ 000$ prvky. Zde bereme otočení o 90 stupňů. Z grafu je patrné, že z libovolné pozice se do výchozí pozice můžeme dostat s maximálně 26 otočeními.

Caleyho graf

Příklad 32

Pro grupu $\mathbb{Z}_6$ *nakreslete Caleyho graf pro množinu generátorů* S.

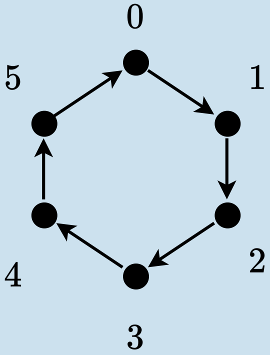
- $S = \{1\}$
- $S = \{2, 3\}$

Caleyho graf

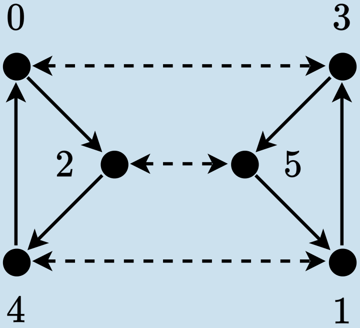
Příklad

Pro grupu $\mathbb{Z}_6$ *nakreslete Caleyho graf pro množinu generátorů* S.

$S = \{1\}$



$S = \{2, 3\}$



Caleyho graf

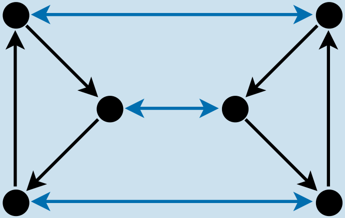
- Můžeme ukázat i naopak, že každý orientovaný graf splňující dříve zmíněné podmínky, je Cayleyho graf pro nějakou grupu.
- Díky symetrii grafu můžeme vybrat označení pro jednotlivé typy hran (např. a, b, $\ldots$) a pojmenovat každý vrchol jakou součin označení hran (případně jejich inverzí) po kterých cestujeme z e do onoho uzlu.

Některé konečné grupy byly prvně zkonstruovány/objeveny použitím grafů.

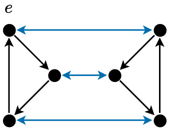
Caleyho graf

Příklad 33

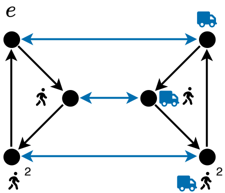
Pro následující graf vytvořte grupu.



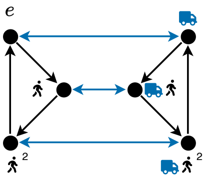
- Zvolíme počáteční uzel e



- Zvolíme označení hran ,
- Pojmenujeme ostatní uzly



Caleyho graf



- Z grafu jednoduše můžeme odvodit tabulku představující operaci.

$*$	e	🚶	🚶^{2}	🚚	🚚🚶	🚚🚶^{2}
e	e	🚶	🚶^{2}	🚚	🚚🚶	🚚🚶^{2}
🚶	🚶	🚶^{2}	e	🚚🚶	🚚🚶^{2}	🚚
🚶^{2}	🚶^{2}	e	🚶	🚚🚶^{2}	🚚	🚚🚶
🚚	🚚	🚚🚶	🚚🚶^{2}	e	🚶	🚶^{2}
🚚🚶	🚚🚶	🚚🚶^{2}	🚚	🚶	🚶^{2}	e
🚚🚶^{2}	🚚🚶^{2}	🚚	🚚🚶	🚶^{2}	e	🚶

Permutace

Definice

Permutace *množiny A je bijekce $\phi : A \to A$.*

Definice

Operaci skládání permutací budeme nazývat **permutační součin***.*
Značíme $\circ$.
Permutační součin je binární operace na kolekci všech permutací A.

Nechť σ a τ jsou permutace množiny A. Složená funkce $\sigma \circ \tau$ definovaná
$A \xrightarrow{\tau} A \xrightarrow{\sigma} A$
je zobrazení z A do A.
Zápis budeme zkracovat na $\sigma\tau$
Všimněte si, že nejprve aplikujeme τ a pak σ. Zápis čteme zprava doleva.

Permutace

Příklad 34

Máme množinu $A = \{1,2,3,4,5\}$. *Na ní máme definovanou permutaci* σ*:*
$1 \to 4,\ 2 \to 2,\ 3 \to 5,\ 4 \to 3,\ 5 \to 1.$
Permutaci můžeme zapsat v kanonickém tvaru následovně:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

Dále máme permutaci τ*:*

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Pak $\sigma\tau$*:*

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

Jak bude vypadat $\tau\sigma$*?*

Permutace

Věta 14

Nechť A je neprázdná množina a S_A je kolekce všech permutací A. Pak S_A s operací permutačního součinu je grupa.

Důkaz

Víme, že složení dvou permutací A dá opět permutaci A, takže S_A je uzavřená na operaci permutačního součinu.
Permutační součin je definován jako složení funkcí, to víme, že je asociativní.
Permutace ι taková, že $\iota(a) = a$, pro všechna $a \in A$ je neutrální prvek.
Pro permutaci σ je inverzní funkce σ^{-1} permutace, která obrací směr zobrazení.
$\sigma^{-1}(a) = a'$ *taková, že* $a = \sigma(a')$ *pro všechna* $a \in A$.
Existence právě jednoho takového prvku je důsledek toho, že σ je bijekce.
$\iota(a) = a = \sigma(a') = \sigma(\sigma^{-1}(a)) = (\sigma\sigma^{-1})(a)$
$\iota(a') = a' = \sigma^{-1}(a) = \sigma^{-1}(\sigma(a')) = (\sigma^{-1}\sigma)(a')$
Takže $\sigma\sigma^{-1}$ i $\sigma^{-1}\sigma$ jsou rovny ι, tedy jsou k sobě inverzní.

Symetrická grupa

Definice

Nechť A je konečná množina $\{1, 2, \ldots, n\}$. Grupa všech permutací A se nazývá **symetrická grupa** *n-prvkové množiny.*
Značíme S_n.

Kolik má S_n prvků?

Symetrická grupa

Definice

Nechť A je konečná množina $\{1, 2, \ldots, n\}$. Grupa všech permutací A se nazývá **symetrická grupa** *n-prvkové množiny.*
Značíme S_n.

Kolik má S_n prvků?

S_n má $n!$ prvků.

Symetrická grupa S_3

Grupa S_3, se skládá ze $3! = 6$ prvků:

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

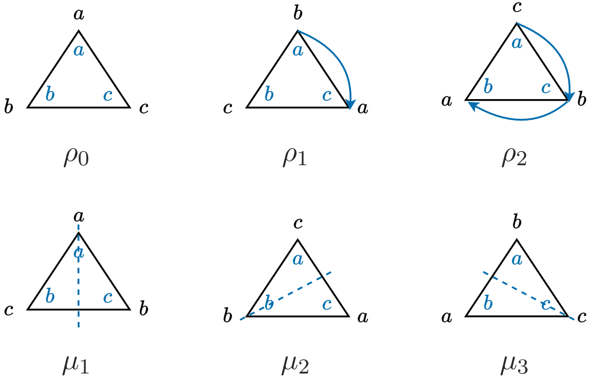
Permutační součin můžeme popsat tabulkou:

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Grupa není abelovská.

Symetrická grupa S_3

Existuje přirozená korespondence mezi prvky S_3 a způsoby, kterými mohou být dvě instance rovnostranného trojúhelníka s vrcholy a, b, c umístěny tak, že jeden překrývá druhý s vrcholy na vrcholech. Proto se S_3 také nazývá **grupa D_3 symetrií rovnostranného trojúhelníka**. D_3 znamená 3. dihedrální grupa. (Obecně D_n je grupa symetrií na pravidelných n-úhelnících)

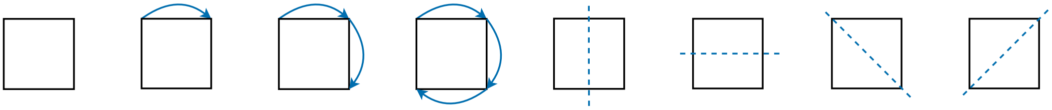


Symetrická grupa D_4

Grupa symetrií čtverce D_4 (oktická grupa)

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$



ρ_0 ρ_1 ρ_2 ρ_3 μ_1 μ_2 δ_1 δ_2

Symetrická grupa D_4

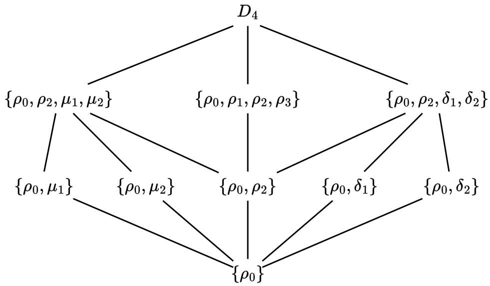
$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_1	μ_2
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_2	μ_1
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Příklad 35

Najděte všechny podgrupy grupy D_4 a nakreslete jejich graf.

Symetrická grupa D_4

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_1	μ_2
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_2	μ_1
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0



Podgrupy

- D_4, $\{\rho_0\}$
- $\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \rho_2\}$, $\{\rho_0, \delta_1\}$, $\{\rho_0, \delta_2\}$
- $\{\rho_0, \rho_2, \mu_1, \mu_2\}$, $\{\rho_0, \rho_1, \rho_2, \rho_3\}$, $\{\rho_0, \rho_2, \delta_1, \delta_2\}$

Caleyho věta

Definice

Nechť $f : A \to B$ *je funkce a* H *je podmnožina* A. **Obor hodnot H při f** *je* $\{f(h) | h \in H\}$. *Značíme* $f[H]$.

Lemma 1

Nechť G *a* G' *jsou grupy a* $\phi : G \to G'$ *je injektivní zobrazení takové, že* $\phi(xy) = \phi(x)\phi(y)$ *pro všechna* $x, y \in G$.
Pak $\phi[G]$ *je podgrupa* G' *a* ϕ *je isomorfismus* G *a* $\phi[G]$.

Důkaz

Ukážeme, že $\phi[G]$ *je grupa.*
Nechť $x', y' \in \phi[G]$. *Pak existují* $x, y \in G$ *takové, že* $\phi(x) = x'$ *a* $\phi(y) = y'$.
Dle předpokladu $\phi(xy) = \phi(x)\phi(y) = x'y'$, *což ukazuje, že* $x', y' \in \phi[G]$ *(uzavřenost).*
Nechť e' *je neutrální prvek z* G'. *Pak*
$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e)$.
Krácení v G' *ukazuje, že* $e' = \phi(e)$, *takže* $e' \in \phi[G]$ *(existence neutrálního prvku).*

Caleyho věta

Důkaz (Pokračování)

Pro $x \in \phi[G]$, *kde* $e' = \phi(e)$, *platí*
$e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1})$
Což ukazuje, že $\phi(x^{-1})$ *je inverzní prvek k* x' *a* $\phi(x^{-1}) \in \phi[G]$ *(inverzní prvky).*
Tedy $\phi[G]$ *je podgrupa* G'.
ϕ *je izomorfismus*
Víme, že ϕ *je injektivní takové, že* $\phi(xy) = \phi(x)\phi(y)$ *pro všechna* $x, y \in G$. *Z čehož isomorfismus přímo vyplývá.*

Caleyho věta

Věta 15

Každá grupa je izomorfní s grupou permutací.

Důkaz

Nechť G *je grupa. Ukážeme, že* G *je isomorfní s podgrupou grupy* S_G.
Dle předchozího lemmatu, stačí najít injektivní zobrazení $\phi : G \to S_G$ *takové, že* $\phi(xy) = \phi(x)\phi(y)$.
Pro $x \in G$, *nechť* $\lambda_x : G \to G$ *je definováno* $\lambda_x(g) = xg$ *pro všechna* $g \in G$ *(násobení zleva prvkem* x*).*
Rovnice $\lambda_x(x^{-1}c) = (x(x^{-1}c) = c$ *pro* $c \in G$ *ukazuje, že* λ_x *zobrazuje* G *na* G *(je surjektivní).*
Pokud $\lambda_x(a) = \lambda_x(b)$, *pak* $xa = xb$ *a díky krácení* $a = b$. *Takže je injektivní a je tedy i permutací* G.

Caleyho věta

Důkaz (Pokračování)

Nyní definujme $\phi : G \to S_G$ *jako* $\phi(x) = \lambda_x$ *pro všechna* $x \in G$.
Chceme ukázat, že je toto zobrazení injektivní. Předpokládejme, že $\phi(x) = \phi(y)$.
Pak $\lambda_x = \lambda_y$. *Dosadíme-li* e: $\lambda_x(e) = \lambda_y(e)$ *a odtud* $xe = ye$ *tedy* $x = y$.
Zbývá ukázat, že $\phi(xy) = \phi(x)\phi(y)$.
Pro každé $g \in G$ *máme* $\lambda_{xy}(g) = (xy)g$. *Permutační součin je funkce skládání, takže*
$(\lambda_x \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg)$.
Takže dle asociativity $\lambda_{xy} = \lambda_x \lambda_y$

Mohli bychom místo násobení prvku zleva použít násobení prvku zprava. Jako procvičení zkuste důkaz upravit.

Reprezentace grupy

Definice

Zobrazení ϕ v důkazu předchozí věty nazýváme **levá pravidelná reprezentace** *grupy G. Zobrazení $\mu : x \to \kappa_x$ takové, že $\kappa_x(g) = gx$, se nazývá* **pravá pravidelná reprezentace** *grupy G.*

Příklad 36

Vypočítejte levou pravidelnou reprezentaci grupy, která je dána tabulkou. (Najděte prvky levé pravidelné reprezentace grupy.)

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Reprezentace grupy

Příklad

Vypočítejte levou pravidelnou reprezentaci grupy, která je dána tabulkou. (Najděte prvky levé pravidelné reprezentace grupy.)

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

- Prvky jsou
  $\lambda_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$, $\lambda_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$, $\lambda_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$
- Tabulka pro tuto reprezentaci (Je stejná jako původní tabulka, jen s přejmenováním $x \to \lambda_x$)

$\circ$	λ_e	λ_a	λ_b
λ_e	λ_e	λ_a	λ_b
λ_a	λ_a	λ_b	λ_e
λ_b	λ_b	λ_e	λ_a

Reprezentace grupy

Příklad

Vypočítejte pravou pravidelnou reprezentaci grupy, která je dána tabulkou. (Najděte prvky pravé pravidelné reprezentace grupy.)

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a