Rád prvku, dihedrálna a symetrická grupa, izmorfizmus grúp

Algebra a diskrétna matematika

Prednáška č. 11

Algebraické štruktúry s jednou binárnou operáciou

Nech M je neprázdna množina a nech platí

(1) $*$ je binárna operácia na M

(2) $*$ je asociatívna na M

(3) $\exists\, e \in M\ \forall x \in M:\ x * e = e * x = x$

(4) $\forall\, x \in M\ \exists x^{-1} \in M:\ x * x^{-1} = x^{-1} * x = e$

Potom dvojicu $(M, *)$ nazývame **grupa**.

Ak sú na M splné iba vlastnosti $(1), (2), (3)$, jedná sa o **monoid**.

Ak na M platí len $(1), (2)$, hovoríme, že $(M, *)$ je **pologrupa**.

Ak na M požadujeme iba platnosť (1), štruktúra $(M, *)$ je **grupoid**.

Rád prvku a grupy $(M, *)$ je najmenšie kladné celé číslo n také, že

$$a^n = e$$

$$a * a * a \dots a * a = e$$

Označuje sa $|a|$.

Ak také n neexistuje, hovoríme, že a má **nekonečný rád**.

Príklad: Určte rády daných prvkov v zodpovedajúcich grupách.

a) všetkých prvkov v $(\mathbb{Z}_6, +)$ mod 6

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$e = 0$ - rád 1

$1 \to$ rád 6, lebo $\overbrace{1+1+1+1+1+1}^{1^6} = 0 \mod 6$

rád
$2 \to 3$
$3 \to 2$
$4 \to 3$
$5 \to 6$

b) prvku 4 v $(\mathbb{Z}, +)$

$e = 0$

$|4| = \infty$

c) komplexnej jednotky i v $(\mathbb{C} - \{(0, 0)\}, \cdot)$

$e = 1$

$|i| = 4$

$i = \sqrt{-1}$
$i^2 = -1$
$i^3 = -i$
$i^4 = (-i)(-i) = 1$

$i^5 = i = \sqrt{-1}$
$i^6 = -1$
$i^7 = -i$
$i^8 = 1$

Množina **generátorov** grupy je taká podmnožina grupy, že každý prvok grupy sa dá vyjadriť ako "súčin" mocnín týchto generátorov.

Prezentácia grupy pomocou generátorov: ⟨ generátory | relácie ⟩

Cyklická grupa je grupa, ktorá je generovaná jedným prvkom g, t. j. je to množina všetkých mocnín prvku g.

Zapisuje sa $\langle g | g^n = e \rangle$, skrátene $\langle g \rangle$.

Príklad: Nájdite generátory grupy $(\mathbb{Z}_5, +)$. $= \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle$

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ + mod 5

$e = 0$

1. $1^1 = 1$

$1^2 = 1 + 1 = 2$

$1^3 = 1 + 1 + 1 = 3$

$1^4 = 1 + 1 + 1 + 1 = 4$

$1^5 = 1 + 1 + 1 + 1 + 1 = 0$

7

áno, 1 je generátor

3. 3

$3 + 3 = 1$

$3 + 3 + 3 = 4$

$3 + 3 + 3 + 3 = 2$

Generátory - Príklad

Príklad: Nájdite generátory grúp $(\mathbb{Z}_6, +), (\mathbb{Z}_5 - \{0\}, \odot)$.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ $+$ mod 6 $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$

$e = 0$

2

$2 + 2 = 4$

$2 + 2 + 2 = 0$

3

$3 + 3 = 0$

$\mathbb{Z}_5 - \{0\} = \{1, 2, 3, 4\}$ $\odot \rightarrow \cdot$ mod 5

$2 \cdot 3 = 1$ mod 5

$e = 1$

2

$2^2 = 4$

$2^3 = 3$

generátor

3

$3^2 = 4$

$3^3 = 2$

generátor

4

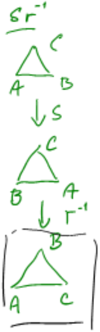
$4^2 = 1$

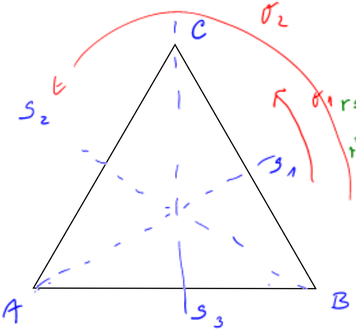
nie je generátor

$(\mathbb{Z}_5 - \{0\}, \odot) = \langle 2 \rangle = \langle 3 \rangle$

Symetrie trojuholníka

Tvorí množina symetrií rovnostranného trojuholníka spolu s operáciou skladania symetrií grupu?





SYMETRIE:

OSOVÉ SYMETRIE

$rs = s_1$ – symetria okolo osi cez A

$r^2 s = s_2$ – " – B

$s = s_3$ – C

$s_1^{-1} = s_1$
$s_2^{-1} = s_2$
$s_3^{-1} = s_3$

GRUPU

OTOČENIA

$r = \sigma_1$ – OTOČENIE OKOLO STREDU o 120^0

$r^2 = \sigma_2$ – 240^0

$e = r^3$ – 360^0

$\sigma_1^{-1} = \sigma_2$

$Sym\Delta = \{e, \sigma_1, \sigma_2, s_1, s_2, s_3\}$

$Sym\Delta = \langle r, s \mid s^2 = e, r^3 = e, rs = sr^{-1} \rangle$

r – otočenie o 120° (σ_1)

s – SYMETRIA PODĽA ZVISLEJ OSI (s_3)

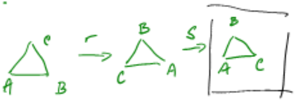
SÚ GENERÁTORY?

$r^2 = \sigma_2$

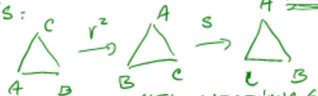
$rs = ?$

$r^2 s = ?$

rs:



$r^2 s$:

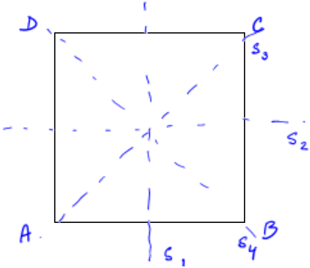


NEKOMUTATÍVNA GR

Symetrie štvorca

Určte grupu symetrií štvorca.

$\mathrm{Sym}\,\square = \{e, \sigma_1, \sigma_2, \sigma_3, s_1, s_2, s_3, s_4\}$



SYMETRIE:

OSOVÉ SYMETRIE

$s = s_1$ – os cez stred strán AB, DC

$r^2 s = s_2$ – os cez ... AD, BC

$rs = s_3$ – uhlopriečka AC

$r^3 s = s_4$ – — " — BD

OTOČENIA

$r = \sigma_1$ – o 90°

$r^2 = \sigma_2$ – o 180°

$r^3 = \sigma_3$ – o 270°

$e = \sigma_4$ – o 360°

$$\boxed{\mathrm{Sym}\,\square = \langle r, s \mid s^2 = e,\ r^4 = e,\ rs = sr^{-1} \rangle}$$

$r = \sigma_1$

$s = s_1$

rs

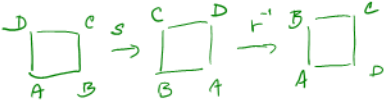
$r^2 s$

$r^3 s$

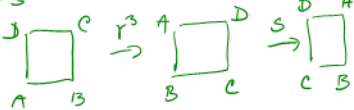
rs:

$r^2 s$:

sr^{-1}



$r^3 s$



Dihedrálna grupa

Grupa symetrií pravidelného n-uholníka sa nazýva **dihedrálna grupa**.

- Označenie: D_n
- Rád: $|D_n| = 2n$
- Neutrálny prvok: e – identita
- Prezentácia: $D_n = \langle r, s | r^n = e, s^2 = e, rs = sr^{-1} \rangle$
  r – rotácia o $360°/n$
  s – symetria podľa pevnej osi symetrie

Príklad: V grupe D_8 zjednodušte prvok $r^5 s r^{-2} s^3 r$.

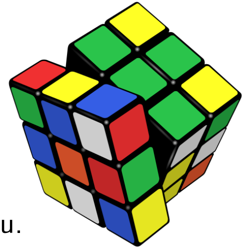
$r^{11} = r^3$

$D_8 = \langle r, s \mid r^8 = e, \ s^2 = e, \ \underline{rs = sr^{-1}} \rangle$

$r^5 s r^{-2} \underset{s \cdot \underset{=e}{s^2}}{s^3} r = r^5 s r^{-2} s r = r^5 \underbrace{s r^{-1}}_{rs} \cdot r^{-1} s r = \underbrace{r^5 \cdot r}_{r^6} \underbrace{s \cdot r^{-1}}_{rs} s r = r^6 r s s r =$

$= r^7 \cdot \underset{e}{s^2} r = r^8 = e$

Grupa Rubikovej kocky $(G, *)$
- štruktúra reprezentujúca hlavolam.



Každý prvok množiny G zodpovedá nejakému pohybu (otočeniu) Rubikovou kockou.

Grupová operácia $*$ je zloženie (následné vykonanie) pohybov kockou.

Rád grupy je $|G| = 43\ 252\ 003\ 274\ 489\ 856\ 000 \approx 4,3 \cdot 10^{19}$

Grupa G je generovaná 6 generátormi - rotáciami 6 stien o $90°$ (v smere hodinových ručičiek).

$$\{C, Z, H, D, L, P\}$$

Najväčší rád prvku je 1260. Jedná sa o prvok $PH^2D^{-1}ZD^{-1}$.

Grupa G nie je abelovská.

Priamy súčin grúp

Priamy súčin dvoch grúp $(S, *)$ a $(T, \circ)$ je definovaný ako operácia $\bullet$ na $S \times T$, kde $\forall s_1, s_2 \in S, t_1, t_2 \in T: \ (s_1, t_1) \bullet (s_2, t_2) = (s_1 * s_2, t_1 \circ t_2)$

Dá sa ukázať, že operácia $\bullet$ je *asociatívna*.

Neutrálny prvok v $(S \times T, \bullet)$ je $e = (e_1, e_2)$, kde e_1 je neutrálny prvok v S a e_2 je neutrálny prvok v T.

Inverzný prvok k prvku (s, t) je prvok (s^{-1}, t^{-1}), pričom s^{-1} je inverzný k s v $(S, *)$ a t^{-1} je inverzný k t v $(T, \circ)$.

Dvojica $(S \times T, \bullet)$ tvorí *grupu*.

Príklad: Určte priamy súčin grúp $(\mathbb{Z}_2, +)$ a $(\mathbb{Z}_2, +)$. $Z_2 = \{0, 1\}$

$Z_2 \times Z_2 = \{\underbrace{(0,0)}_{e}, (0,1), (1,0), (1,1)\}$

$(0,1) \bullet (1,0) = (\underset{mod 2}{0+1}, \underset{mod 2}{1+0}) = (1,1)$

$(0,1) \bullet (1,1) = (1, 0)$

$(0,1)^{-1} = (0,1)$

$(1,0)^{-1} = (1,0)$

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

grupa

Príklad

Vytvorte priamy súčin grúp $(\mathbb{Z}_2, \overset{\text{mod } 2}{+})$ a $(\mathbb{Z}_3, \overset{\text{mod } 3}{+})$.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{\underset{e}{(0,0)}, (0,1), (0,2), (1,0), (1,1), (1,2)\}$$

rády: 1 3 3 2 6 6

$$(0,2) \circ (1,1) = (\underset{\text{mod } 2}{0+1}, \underset{\text{mod } 3}{2+1}) = (1,0)$$

$$(1,0) \circ (1,2) = (0,2)$$

$$(1,1) \circ (1,2) = (0,0)$$

$$(0,1)^{-1} = (0,2)$$
$$(0,2)^{-1} = (0,1)$$
$$(1,0)^{-1} = (1,0)$$
$$(1,1)^{-1} = (1,2)$$
$$(1,2)^{-1} = (1,1)$$

Izomorfizmus grúp

Nech $(M_1, *)$ a $(M_2, \circ)$ sú dve grupy. Ak existuje bijekcia φ medzi M_1 a M_2 taká, že $\forall x, y \in M_1$ platí

$$\varphi(x * y) = \varphi(x) \circ \varphi(y),$$

potom grupy $(M_1, *)$ a $(M_2, \circ)$ sú **izomorfné**, píšeme $M_1 \cong M_2$. Zobrazenie φ sa nazýva **izomorfizmus**.

Neformálne: Dve grupy sú izomorfné, ak majú "takú istú štruktúru".

Izomorfné grupy majú rovnaký rád a rovnaký počet prvkov určitého rádu.

Všetky grupy s jedným prvkom sú izomorfné.

Tvrdenie

Existuje konečne veľa grúp daného konečného rádu (až na izomorfizmus).

Jedným zo základných problémov konečnej teóre grúp je ich klasifikovať.

Príklad

Príklad: Rozhodnite, či sú niektoré z grúp $\mathbb{Z}_6, D_3$ a $\mathbb{Z}_2 \times \mathbb{Z}_3$ izomorfné.

$Z_6 = \{\underset{e}{0}, 1, 2, 3, 4, 5\}$

rády 1 6 3 2 3 6

$D_3 = \{e, r, r^2, s, rs, r^2s\}$

rády 1 3 3 2 2 2

$D_3 \not\cong Z_6$ $\quad D_3 \not\cong Z_2 \times Z_3$

$Z_2 \times Z_3 = \{\underset{e}{(0,0)}, \underline{(0,1)}, \underline{(0,2)}, (1,0), (1,1), (1,2)\}$

rády 1 3 3 2 6 6

MEDZI Z_6 a $Z_2 \times Z_3$ BY MOHOL EXISTOVAŤ IZOMORFIZMUS

+mod 6 $\quad$ (mod 2, mod 3)

$\varphi(x + y) = \varphi(x) \bullet \varphi(y)$

HĽADÁME HO:

$\varphi: Z_6 \to Z_2 \times Z_3$?

$\varphi:$
$0 \to (0,0)$
$1 \to (1,1)$ (lebo je rádu 6)
$2 \to (0,2)$
$3 \to (1,0)$
$4 \to (0,1)$
$5 \to (1,2)$

$\varphi(2) = \varphi(1+1) = \varphi(1) \bullet \varphi(1) = (1,1) \bullet (1,1) = (0,2)$

$\varphi(3) = \varphi(1+2) = \varphi(1) \bullet \varphi(2) = (1,1) \bullet (0,2) = (1,0)$

$\varphi(4) = \varphi(2+2) = \varphi(2) \bullet \varphi(2) = (0,2) \bullet (0,2) = (0,1)$

$\varphi(5) = \varphi(2+3) = \varphi(2) \bullet \varphi(3) = (0,2) \bullet (1,0) = (1,2)$

áno sú izomorfné $\quad \boxed{Z_2 \times Z_3 \cong Z_6}$

$+ \bmod 4$ $\qquad\qquad$ $\cdot \bmod 5$

Príklad: Sú grupy $(\mathbb{Z}_4, +)$ a $(\mathbb{Z}_5 - \{0\}, \cdot)$ izomorfné?

$2^2 = 4$

$2^3 = 8 \equiv 3 \bmod 5$

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

e: 1 4 2 4

rády

$\mathbb{Z}_5 - \{0\} = \{1, 2, 3, 4\}$

e: 1 4 4 2

$\Downarrow$

$2^4 = 16 \equiv 1 \bmod 5$

$3^4 = 81 \equiv 1 \bmod 5$

$3^2 = 9 \equiv 4 \bmod 5$

$3^3 = 27 \equiv 2 \bmod 5$

$4^2 = 16 \equiv 1 \bmod 5$

$\varphi : \mathbb{Z}_4 \to \mathbb{Z}_5 - \{0\}$?

$\varphi : 0 \to 1$

$1 \to 2$

$2 \to \varphi(2) = \varphi(1+1) = \varphi(1) \cdot \varphi(1) = 2 \cdot 2 = 4$

$3 \to \varphi(3) = \varphi(1+2) = \varphi(1) \cdot \varphi(2) = 2 \cdot 4 = 3$

$(\mathbb{Z}_4, +) \cong (\mathbb{Z}_5 - \{0\}, \cdot)$

Permutácie a ich skladanie

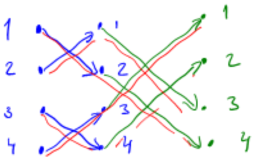
$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 1 & 5 & 4 & 6 & 2 & 7 \end{pmatrix} = (18723)(45)(6) = (18723)(45)$$

Identická permutácia – $id = (1)(2)(3)\dots(n)$.

Skladanie permutácií – *zľava doprava*.

Príklad: Zložte dané permutácie

$(12)(34) \circ (13)(24)$ = $(14)(23)$



$(13)(24) \circ (12)(34)$ = $(14)(23)$

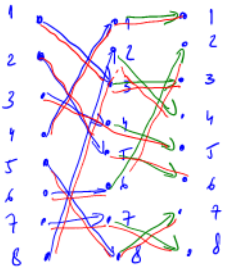
Príklad: Zložte dané permutácie

$(12345) \circ (13524)$ $= (1\,4\,2\,5\,3)$

$(13524) \circ (12345)$ $= (1\,4\,2\,5\,3)$

$(134)(258) \circ (2456)(78)$ $= (1\,3\,5\,7\,8\,4)(2\,6)$

$(2456)(78) \circ (134)(258)$ $= (1\,3\,4\,8\,7\,2)(5\,6)$



NEKOMUTATÍVNE
(NEABELOVSKÉ)

Symetrická grupa

Nech $X = \{1, 2, \ldots, n\}$ a nech S_n je množina všetkých bijekcií (čiže permutácií) $\sigma : X \to X$. Potom platí

- zloženie dvoch bijekcií je bijekcia
- skladanie bijekcií je asociatívne
  $(\sigma \circ \tau) \circ \pi(x) = (\sigma \circ \tau)(\pi(x)) = \sigma(\tau(\pi(x)) = \sigma(\tau \circ \pi)(x) = \sigma \circ (\tau \circ \pi)(x)$
- identické zobrazenie je bijekcia na X $= e$
- inverzné zobrazenie bijekcie v S_n je tiež bijekcia v S_n

Množina S_n všetkých permutácií n objektov spolu s operáciou skladania permutácií tvorí grupu rádu $n!$ a nazýva sa **symetrická grupa** rádu n.

Symetrická grupa S_n - množina všetkých permutácií n objektov s operáciou skladania permutácií.

Neutrálny prvok: $e = id = (a_1)(a_2)\dots(a_n)$

Inverzný prvok: $(a_1a_2a_3a_4\dots a_{n-1}a_n)^{-1} = (a_1a_na_{n-1}\dots a_4a_3a_2)$

$((a_1a_2a_3\dots a_{i-1}a_i)(b_1b_2\dots b_j))^{-1} = (a_1a_ia_{i-1}\dots a_3a_2)(b_1b_j\dots b_2)$

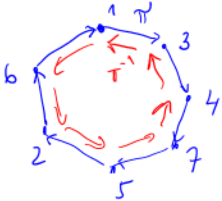
Príklad: K daným prvkom nájdite inverzné prvky

$\pi = (1347526)$ $\quad\pi^{-1} = (1625743)$

(625741) ✓

$\varphi = (1548)(23769)$ $\quad\varphi^{-1} = (1845)(29673)$

$\chi = (1532)(48)(697)$ $\quad\chi^{-1} = (1235)(48)(679)$



Príklad

Vypíšte všetky prvky symetrickej grupy S_3 a overte komutatívnosť.
Zistite, či je izomorfná s niektorou známou grupou rovnakého rádu.

$|S_3| = 3! = 6$

$S_3 = \{ e, (12), (13), (23), (123), (132) \}$

rády: 1 2 2 2 3 3

(123)

$(12) \circ (12) = (1)(2)$

$(123) \circ (123) = (132)$

$(123)^3 = (123) \circ (132) = (1)(2)(3) = e$

Príklad

Aké rôzne rády majú prvky grupy S_5?

Existuje nejaký súvis medzi prvkami grupy S_5 a prvkami grupy D_5?

$|S_5| = 5! = 120$

rád

1: $e = id$ ->

2: $(1\,2)$

alebo

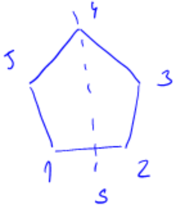
$(1\,2)(3\,5)$

3: $(1\,2\,5)$

4: $(1\,3\,4\,2)$

5: $(1\,3\,5\,2\,4)$

6: $(1\,2\,3)(4\,5)$



$s = (1\,2)(3\,5)$

$r = (1\,2\,3\,4\,5)$