Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

Prehľad z 11. prednášky

Dihedrálna, symetrická grupa, izmorfizmus grúp

Algebraické štruktúry s jednou binárnou operáciou

Nech M je neprázdna množina a nech platí

(1) $*$ je binárna operácia na M

(2) $*$ je asocitívna 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

$$a^n = e,$$

$$(a * a * a \ldots a * a = e)$$

.

Označuje sa $|a|$.

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

Príklad 1: Určte rády daných prvkov v zodpovedajúcich grupách.

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

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

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

Odpoveď: a) rád 0 je 1 (jedná sa o neutrálny prvok), rády prvkov $1, 2, 3, 4, 5$ sú $6, 3, 2, 3, 6$ v zodpovedajúcom poradí; b) ∞, c) 4

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

Prezentácia grupy pomocou generátorov: $\langle$ generátory$|$ relácie $\rangle$

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 $\langle g\rangle$.

Grupa z príkladu 7 je cyklická grupa $(\mathbb{Z}_2, +)$ a grupa z príkladu 8 je $(\mathbb{Z}_3, +)$.

Príklad 2: Nájdite generátory grúp $(\mathbb{Z}_5, +), (\mathbb{Z}_6, +), (\mathbb{Z}_5 - \{0\}, \odot)$.

Odpoveď:
$(\mathbb{Z}_5, +) = \langle 1\rangle = \langle 2\rangle = \langle 3\rangle = \langle 4\rangle$
$(\mathbb{Z}_6, +) = \langle 1\rangle = \langle 5\rangle$
$(\mathbb{Z}_5 - \{0\}, \odot) = \langle 2\rangle = \langle 3\rangle$

Dihedrálna grupa

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

Označuje sa D_n

Jej rád je $|D_n| = 2n$ (n osových symetrií a n otočení)

Neutrálny prvok e je 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

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_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 3: Priamy súčin grúp $(\mathbb{Z}_2,+)$ a $(\mathbb{Z}_2,+)$ je množina
$\mathbb{Z}_2\times\mathbb{Z}_2=\{(0,0),(0,1),(1,0),(1,1)\}$
s operáciou súčtu modulo 2 v oboch súradniciach.
Napr. $(0,1)\oplus(1,0)=(1,1),(1,1)\oplus(1,0)=(0,1),(1,0)\oplus(1,1)=(0,1)$ atď.

Príklad 4: Priamy súčin grúp $(\mathbb{Z}_2,+)$ a $(\mathbb{Z}_3,+)$ je množina
$\mathbb{Z}_2\times\mathbb{Z}_3=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$
s operáciou $\oplus$, ktorá vykoná súčet modulo 2 v prvej súradnici a súčet modulo 3 v druhej súradnici.
Napr. $(1,2)\oplus(0,2)=(1,1),\quad(1,1)\oplus(1,2)=(0,0)$.

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.

Tvrdenie 1: Všetky grupy s jedným prvkom sú izomorfné.

Tvrdenie 2: Existuje konečne veľa grúp daného konečného rádu (až na izomorfizmus).

Príklad 5: Grupy $(\mathbb{Z}_4,+)$ a $\mathbb{Z}_2\times\mathbb{Z}_2$ nie sú izomorfné, pretože grupa $(\mathbb{Z}_4,+)$ má dva prvky rádu 4 a také sa v $\mathbb{Z}_2\times\mathbb{Z}_2$ nenachádzajú. Všetky jej prvky majú rád 2.

Príklad 6: Rozhodnite, či sú niektoré z grúp $\mathbb{Z}_6, D_3$ a $\mathbb{Z}_2\times\mathbb{Z}_3$ izomorfné.

Odpoveď: Overením rádov prvkov zistíme, že D_3 nemôže byť izomorfná ani

s $\mathbb{Z}_6$ ani s $\mathbb{Z}_2 \times \mathbb{Z}_3$.
V grupách $\mathbb{Z}_6$ a $\mathbb{Z}_2 \times \mathbb{Z}_3$ má rovnaký počet prvkov zhodné rády. Príslušný izomorfizmus je $\varphi(0) = (0,0), \varphi(1) = (1,1), \varphi(2) = (0,2), \varphi(3) = (1,0), \varphi(4) = (0,1), \varphi(5) = (1,2)$.

Príklad 7: Sú grupy $(\mathbb{Z}_4, +)$ a $(\mathbb{Z}_5 - \{0\}, \cdot)$ izomorfné?

Odpoveď: Áno

Symetrická grupa

Skladanie permutácií vykonávame *zľava doprava.*

Príklad 8: Zložte dané permutácie

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

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

$(134)(258) \circ (2456)(78) = (135784)(26)$

$(2456)(78) \circ (134)(258) = (134872)(56)$

Vo všeobecnosti je skladanie permutácií nekomutatívne, ale máme výnimky.

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
- 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** stupňa n.

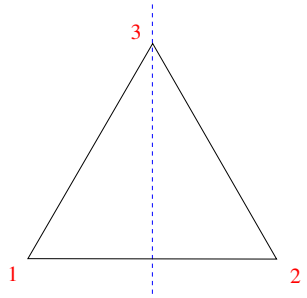
Inverzný prvok sa počíta nasledujúcim spôsobom
$(a_1 a_2 a_3 a_4 \ldots a_{n-1} a_n)^{-1} = (a_1 a_n a_{n-1} \ldots a_4 a_3 a_2)$
$((a_1 a_2 a_3 \ldots a_{i-1} a_i)(b_1 b_2 \ldots b_j))^{-1} = (a_1 a_i a_{i-1} \ldots a_3 a_2)(b_1 b_j \ldots b_2)$

Príklad 9: Vypíšte všetky prvky symetrickej grupy S_3 a overte komutatívnosť. Zistite, či je izomorfná s niektorou známou grupou rovnakého rádu.

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

Komutatívnosť neplatí; napr. $(12)(123) \neq (123)(12)$.

S_3 je izomorfná s dihedrálnou grupou $D_3 = \{e, r, r^2, s, rs, r^2s\}$, kde r je rotácia okolo stredu o $120°$ proti smeru hodinových ručičiek a s je osová symetria podľa zvislej osi.



Zodpovedajúci izomorfizmus $\varphi : S_3 \to D_3$ je
$\varphi(e) = e, \varphi((123)) = r, \varphi((132)) = r^2,$
$\varphi((12)) = s, \varphi((23)) = rs, \varphi((13)) = r^2s$

Príklad 10: Aké rôzne rády majú prvky grupy S_5?

Odpoveď: Rád 1 má identita,
rád 2 majú prvky typu (ij), $i, j \in \{1, 2, 3, 4, 5\}$, $i < j$
rád 2 majú tiež prvky typu $(ij)(k\ell)$, $i, j, k, \ell \in \{1, 2, 3, 4, 5\}, i < j, k < \ell$,
rád 3 majú prvky tvaru (ijk), $i, j, k \in \{1, 2, 3, 4, 5\}$, $i < j, k$
rád 4 majú prvky $(ijk\ell)$, $i, j, k, \ell \in \{1, 2, 3, 4, 5\}$, $i < j, k, \ell$,
rád 5 majú prvky $(1ijk\ell)$, $i, j, k, \ell \in \{2, 3, 4, 5\}$,
rád 6 majú prvky tvaru $(1i)(jk\ell)$, $i, j, \ell \in \{2, 3, 4, 5\}$, $j < k, \ell$,
pričom prvky i, j, k, ℓ sú vždy navzájom rôzne.

Permutácia zamieňajúca dva prvky a fixujúca všetky ostatné sa nazýva **transpozícia**.

Každú permutáciu je možné napísať vo forme súčinu transpozícií.

$$(a_1a_2a_3a_4 \dots a_n) = (a_1a_2)(a_1a_3)(a_1a_4) \dots (a_1a_n)$$

Permutácia je **párna**, ak je súčinom párneho počtu transpozícií.

Permutácia je **nepárna**, ak je súčinom nepárneho počtu transpozícií.

Príklad 11: Určte paritu daných permutácií

a) (13587)

b) (245398)

c) (142)(3875)

Odpoveď: a) párna permutácia, lebo (13587) = (13)(15)(18)(17)
b) nepárna permutácia; (245398) = (24)(25)(23)(29)(28)
c) nepárna permutácia; (142)(3875) = (14)(12)(38)(37)(35)

Množina všetkých párnych premutácií n prvkovej množiny spolu s operáciou skladania permutácií tvorí grupu, ktorá sa nazýva **alternujúca grupa** stupňa n a označuje sa A_n.

Počet prvkov A_n je $\frac{n!}{2}$.

Príklad 12: Vypíšte všetky prvky grupy A_3 a grupy A_4.

Odpoveď: $A_3 = \{e, (123), (132)\}$
$A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$