Algebra a diskrétna matematika
Prehľad z 12. týždňa
Izmorfizmus grúp, symetrické grupy, polia

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**.

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 1: 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 2: 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).

Jedným zo základných problémov konečnej teóre grúp je ich klasifikovať.

Príklad 3: 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 4: 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 5: Sú grupy $(\mathbb{Z}_4, +)$ a $(\mathbb{Z}_5 - \{0\}, \cdot)$ izomorfné?

Odpoveď: Áno

Symetrická grupa

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

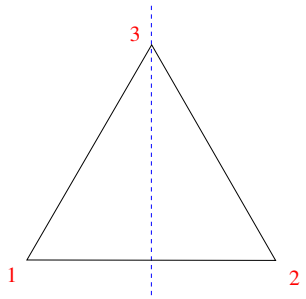
- zloženie dvoch bijekcií je bijekcia
- skladanie bijekcií je asociatívne
$(\sigma \circ \tau) \circ \pi(x) = (\sigma \circ \tau)(\pi(x)) = \sigma(\tau(\pi(x)) = \sigma(\tau \circ \pi)(x) = \sigma \circ (\tau \circ \pi)(x)$
- identické zobrazenie je bijekcia na X
- inverzné zobrazenie bijekcie v S_n 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
$(a_1a_2a_3a_4 \ldots a_{n-1}a_n)^{-1} = (a_1a_na_{n-1} \ldots a_4a_3a_2)$

Príklad 6: 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° v smere 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 7: 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.

Alternujúca grupa

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 8: 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 9: Vypíšte všetky prvky grupy A_3 a grupy A_4.

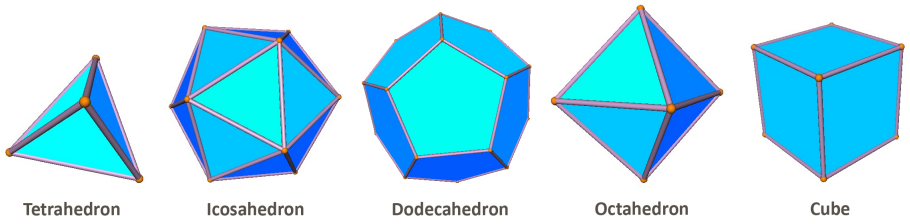
Odpoveď: $A_3 = \{e, (123), (132)\}$

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

Platónske telesá

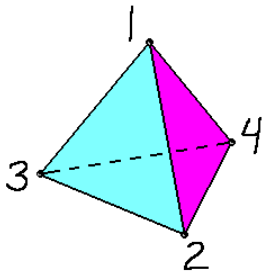
Platónske teleso je mnohosten tvorený pravidelnými zhodnými mnohouholníkmi.

Existuje len 5 nasledujúcich platónskych telies.



štvorsten dvadsať sten dvanásť sten osemsten kocka

Príklad 10: Určte grupu rotácií pravidelného štvorstena.



Odpoveď: Prvky grupy sú:
- identita,
- 8 prvkov rádu 3 – otočenia okolo 4 osí prechádzajúcich cez vrchol a stred protiľahlej steny o 120° a 240°,
- 3 prvky rádu 2 – otočenia okolo 3 osí prchádzajúcich stredmi protiľahlých hrán o 180°.

Grupa rotácií pravidelného štvorstena je izomorfná s grupou A_4.

Príklad 11: Určte grupu rotácií kocky.

Odpoveď: Prvky grupy sú:
- identita,
- 8 prvkov rádu 3 – otočenia okolo 4 telesových uhlopriečok o 120° a 240°,
- 9 prvkov rádu 4 – otočenia okolo 3 osí prechádzajúcich stredmi protiľahlých stien o $90°, 180°$ a $270°$
- 6 prvkov rádu 2 – otočenia okolo 6 osí prechádzajúcich stredmi protiľahlých hrán o $180°$.

Grupa rotácií kocky je izomorfná s grupou S_4.

Polia

Medzi slávne antické problémy, ktoré sa viac ako dvetisíc rokov nedarilo vyriešiť patria:

• *Problém trisekcie uhla* – Pomocou pravítka a kružidla zostrojte uhol, ktorý je tretinou daného uhla.

• *Problém kvadratúry kruhu* – Pomocou pravítka a kružidla zostrojte štvorec, ktorý má rovnaký obsah ako daný kruh.

• *Problém zdvojenia kocky* – Pomocou pravítka a kružidla zostrojte kocku, ktorá má dvojnásobný objem ako daná kocka.

Odpoveď o ich neriešiteľnosti priniesla až moderná algebra v 19. storočí. Pomocou prostriedkov algebry sa dá dokázať, že pomocou pravítka a kružidla nedokážeme žiadnou konštrukciou
− rozdeliť daný uhol na tri rovnaké časti,
− zostrojiť z úsečky dĺžky 1 úsečku dĺžky π,
− zostrojiť z úsečky dĺžky a úsečku dĺžky $a\sqrt[3]{2}$.

Dôležitá algebraická štruktúra v tomto dôkaze je **pole**.

Pole je množina F s dvoma binárnymi operáciami $\oplus, \otimes$, pričom sú splnené nasledujúce podmienky

- $(F, \oplus)$ a $(F - \{0\}, \otimes)$ tvoria komutívne grupy,
- Na F platí distributívny zákon

$$\forall\ a, b, c \in F: \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

Operácie $\oplus, \otimes$ zvyčajne nazývame *sčitovanie* a *násobenie*.

Pole potom jednoducho zapisujeme $(F, +, \cdot)$.
Grupa $(F, +)$ sa nazýva *aditívnou* grupou poľa, skrátene F^+.
Grupa $(F - \{0\}, \cdot)$ sa nazýva *multiplikatívnou* grupou poľa, skrátene $F^\times$.

Príklad 12: Najznámejšie nekonečné polia sú $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$.

Príklad 13: Príklad konečného poľa je $(\mathbb{Z}_5, +, \cdot)$.
Jeho aditívny neutrálny prvok je 0 a inverzné prvky v aditínej grupe sú $-1 = 4, -2 = 3, -3 = 2, -4 = 1$.
Multiplikatívny inverzný prvok je 1 a inverzné prvky v multiplikatívnej grupe sú $2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$.
Rovnicu $3x + 4 \equiv 1$ v $\mathbb{Z}_5$ riešime nasledovne

$$\begin{aligned} 3x + 4 + 1 &= 1 + 1 \\ 3x &= 2 \\ 3^{-1} \cdot 3x &= 3^{-1} \cdot 2 \\ 2 \cdot 3x &= 2 \cdot 2 \\ x &= 4 \end{aligned}$$

Príklad 14: V poli $(\mathbb{Z}_5, +, \cdot)$ riešte rovnicu

$$x^2 + 4x + 3 = 0$$

Odpoveď: $x_1 = 2, x_2 = 4$

Príklad 15: V poli $\mathbb{Z}_5$ riešte sústavu rovníc

$$\begin{aligned} 3x + \ \ y &= 3 \\ x + 3y &= 2 \end{aligned}$$

Odpoveď: $x = 4, y = 1$

Príklad 16: V $\mathbb{Z}_6$ rovnica $3x + 4 = 2$ nemá riešenie, lebo k 3 neexistuje multiplikatívny inverz. $\mathbb{Z}_6$ nie je pole!

Tvrdenie 3: Ak p je prvočíslo, tak pre každé $x \in \mathbb{Z}_p - \{0\}$ existuje $y \in \mathbb{Z}_p - \{0\}$ také, že $x \cdot y \equiv 1 \pmod{p}$.

Aditívnym rádom prvku x poľa $(F, +, \cdot)$ je najmenšie prirodzené číslo n, pre ktoré platí $n \cdot x = 0$; ak také n neexistuje, rádom prvku x je ∞.

Tvrdenie 4: V každom poli majú všetky prvky ($\neq 0$) rovnaký aditívny rád.

Multiplikatívnym rádom prvku x poľa $(F, +, \cdot)$ je najmenšie prirodzené číslo n, pre ktoré platí $x^n = 1$; ak také n neexistuje, rádom prvku x je ∞.

Rád poľa je počet prvkov poľa.

Tvrdenie 5: Rád konečného poľa je mocnina prvočísla.

Tvrdenie 6: Pre každé prvočíslo p a prirodzené číslo n existuje práve jedno (až na izomorfizmus) pole rádu $p^n = q$.
Toto pole sa nazýva **Galoisove pole** a označuje sa $GF(q)$.