Algebra a diskrétna matematika

doc. RNDr. Jana Šiagiová, PhD.

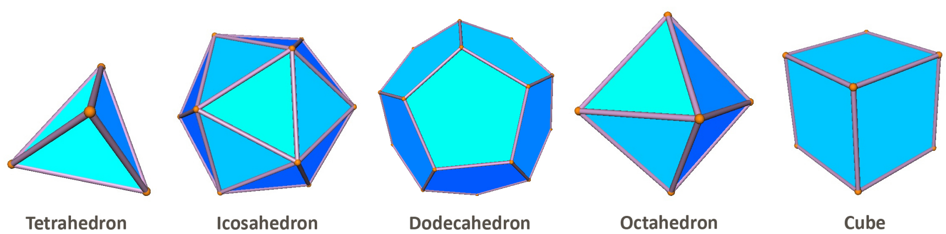
Prehľad z 12. prednášky

Platónske telesá, polia

Platónske telesá

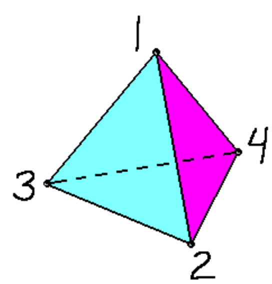
Platónske teleso je pravidelný mnohosten tvorený pravidelnými zhodnými mnohouholníkmi.

Existuje len 5 nasledujúcich platónskych telies.



štvorsten dvadsaťsten dvanásťsten osemsten kocka

Príklad 1: 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 prechádzajúcich stredmi protiľahlých hrán o 180°.

Grupa rotácií pravidelného štvorstena je 12 prvková podgrupa grupy S_4.

Príklad 2: Určte grupu rotácií kocky.

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

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 komutatívne 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 3: Najznámejšie nekonečné polia sú $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$.

Príklad 4: 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 5: V poli $(\mathbb{Z}_5, +, \cdot)$ riešte rovnicu

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

Odpoveď: $x_1 = 2, x_2 = 4$

Príklad 6: V poli $\mathbb{Z}_5$ riešte sústavu rovníc

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

Odpoveď: $x = 4, y = 1$

Príklad 7: V $\mathbb{Z}_6$ rovnica $3x + 4 = 2$ nemá riešenie, lebo k 3 neexistuje multiplikatívny inverz. $\mathbb{Z}_6$ nie je pole!

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

Rád poľa je počet prvkov poľa.

Tvrdenie 2: Rád konečného poľa je mocnina prvočísla.

Tvrdenie 3: 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 $GF(q)$.

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 ∞.

Príklad 8: Vypočítajte aditívne a mutliplikatívne rády prvkov $2, 3$ v poli $\mathbb{Z}_{11}$.

Odpoveď: Aditívny rád prvku 2 je 11, pretože najmenšie n, ktoré vyhovuje rovnici $n \cdot 2 \equiv 0 \pmod{11}$, je $n = 11$. To isté platí pre prvok 3.

Multiplikatívny rád prvku 2 je 10, pretože $2^{10} \equiv 1 \pmod{11}$ a 10 je najmenšia taká kladná mocnina.
Prvok 3 má multiplikatívny rád 5, lebo $3^5 \equiv 1 \pmod{11}$ a 5 je najmenšia taká kladná mocnina.

Príklad 9: Ktorý prvok generuje pole $\mathbb{Z}_{17}$?

Odpoveď: Ak prvok x je generátor v $\mathbb{Z}_{17}$, potom platí
$x^{16} \equiv 1$ a $x^8 \equiv -1 \pmod{16}$.

Postupne ideme overovať mocniny prvkov v $\mathbb{Z}_{17}$.
$2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16 \equiv -1, 2^8 \equiv 1$, teda 2 nie je generátor $\mathbb{Z}_{17}$.

$3^2 \equiv 9, 3^3 \equiv 10, 3^4 \equiv 13, 3^5 \equiv 5, 3^6 \equiv 15, 3^7 \equiv 11, 3^8 \equiv 16 \equiv -1,$

$3^9 \equiv 3 \cdot 3^8 \equiv -3 \equiv 14, 3^{10} \equiv -3 \cdot 3 \equiv 8, 3^{11} \equiv 7, 3^{12} \equiv 4, 3^{13} \equiv 12, 3^{14} \equiv 2, 3^{15} \equiv 6, 3^{16} \equiv 1.$

Prvok 3 je generátor poľa $\mathbb{Z}_{17}$.

Grupa je cyklická, ak je generovaná jedným prvkom.

Veta: Multiplikatívna grupa každého *konečného* poľa je **cyklická**.

Každý generátor multiplikatívnej grupy poľa nazývame **primitívny prvok**.

Nájsť primitívny prvok v poli nie je triviálne, ak ide o pole veľkého rádu.

Príklad 10: V poli $\mathbb{Z}_{23}$ nájdite primitívny prvok.

Odpoveď: Hľadáme prvok x v $\mathbb{Z}_{23}$, pre ktorý $x^{22} \equiv 1 \pmod{23}$ a tiež $x^{11} \equiv -1 \equiv 22 \pmod{23}$.

$2^{11} \equiv 1 \pmod{23}$, 2 nie je generátor. To isté platí pre 4.

Overíme prvok 3.
$3^3 \equiv 4$, takže $3^{33} \equiv (3^3)^{11} \equiv 4^{11} \equiv 1 \pmod{23}$ (*)
Ale potom ak by 3 bol primitívny prvok, tak 3^{11} by musel byť $-1 \pmod{23}$, a teda
$3^{33} = 3^{22} \cdot 3^{11} \equiv 1.(-1) \equiv -1 \bmod 23$, čo je v rozpore s (*).
Ani 3 nie je primitívnym prvkom v $\mathbb{Z}_{23}$.

Overme prvok 5.
$5^2 \equiv 2, 5^{10} \equiv 2^5 \equiv 9, 5^{11} \equiv 9 \cdot 5 \equiv -1 \pmod{23}$.
Prvok 5 je primitívny v poli $\mathbb{Z}_{23}$.

Počet primitívnych prvkov

Pole rádu p má $\varphi(p-1)$ primitívnych prvkov, kde φ je Eulerova funkcia (počet kladných čísel menších ako $p-1$ a nesúdeliteľných s $p-1$).

Ak prirodzené číslo n má prvočíselný rozklad $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, potom

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

Príklad 11: Určte počet primitívnych prvkov v poliach $\mathbb{Z}_{11}, \mathbb{Z}_{17}, \mathbb{Z}_{19}$.

Odpoveď:

$\varphi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5}) = 4$
$\varphi(16) = 16(1 - \frac{1}{2}) = 8$
$\varphi(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 6$
V poli $\mathbb{Z}_{11}$ sú 4 primitívne prvky, v poli $\mathbb{Z}_{17}$ je ich 8 a pole $\mathbb{Z}_{19}$ ich má 6.

Príklad 12: Určte, ktoré prvky majú v poli $\mathbb{Z}_{19}$ druhé odmocniny.

Odpoveď: Najprv je potrebné nájsť primitívny prvok v $\mathbb{Z}_{19}$. Sú nimi napríklad prvky 2 a 3. Potom všetky prvky, ktoré sú párne mocniny primitívneho prvku, majú v $\mathbb{Z}_{19}$ druhú odmocninu.
Túto množinu tvoria prvky $1, 4, 5, 6, 7, 9, 11, 16, 17$.

Príklad 13: Riešte rovnicu $x^3 = 1$ v poli $\mathbb{Z}_7$ a v poli $\mathbb{Z}_{11}$.

Odpoveď: V $\mathbb{Z}_7$ sú korene $x_1 = 1, x_2 = 2, x_3 = 4$.
V poli $\mathbb{Z}_{11}$ je iba jeden koreň $x = 1$, pretože $11 - 1$ nie je deliteľné číslom 3.

Malá Fermatova veta: Nech p je prvočíslo a nech a je celé číslo nesúdeliteľné s p. Potom platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dôkaz: Budeme dokazovať ekvivalentné tvrdenie $a^p \equiv a \pmod{p}$.

Matematickou indukciou vzhľadom na a, pričom p je prvočíslo a $p \nmid a$.

1. $a = 2$

$$2^p = (1+1)^p = \binom{p}{0} + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + \binom{p}{p} = 2 \pmod{p}$$

Využili sme tu fakt, že pre $k < p$ je $\binom{p}{k} \equiv 0 \pmod{p}$.

2. Predpokladajme, že platí $a^p \equiv a \pmod{p}$.

Ukážeme, že platí aj $(a+1)^p \equiv a + 1 \pmod{p}$.

$$(a+1)^p = \binom{p}{0} a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + \binom{p}{p} \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

Príklad 14: Bez použitia kalkulačky vypočítajte

a) $19669^{28} \pmod{29}$

b) $3321^{3323} \pmod{3323}$

c) $11^{209458} \pmod{104729}$

Odpoveď: Keďže každé z čísel $29, 3323, 104729$ je prvočíslo, je možné aplikovať Malú Fermatovu vetu.

a) $19669^{28} \equiv 1 \pmod{29}$

b) $3321^{3323} \equiv 3321 \pmod{3323}$

c) $11^{209458} = (11^{104728})^2 \cdot 11^2 \equiv 121 \pmod{104729}$

Veľká Fermatova veta: Pre žiadne nenulové celé čísla a, b, c a $n > 2$ *neplatí*

$$a^n + b^n = c^n$$

Považuje sa za jeden z najťažších matematických problémov.
V roku 1637 Fermat napísal toto tvrdenie na okraj jedného listu Diofantovej Aritmetiky (3. st. pnl) s tým, ze údajný dôkaz sa mu tam už nezmestil.
Prvý dôkaz publikoval v roku 1995 anglický matematik Andrew Wiles.
V tom istom roku s Richardom Taylorom odstránili medzeru v dôkaze.