Teorie grup 1
Příklad axiomatické teorie

Alena Šolcová

Binární operace Binary operation

- Binární operací na neprázdné množině *A* rozumíme každé zobrazení kartézského součinu *A* x *A* do *A*.
- Multiplikativní zápis operace
- Aditivní zápis operace
- Cayleyho (Cayleyova) tabulka - pro binární operaci na konečné množině
- Binární operace na nekonečných množinách zadáváme nějakým předpisem nebo zákonitostí.

Příklady binárních operací □, ○

Příklad 1: Nechť A je neprázdná množina

A= {a, b, c}.

Tabulkami definujeme operace □, ○

a □ a = c

b □ c = b

c □ a = a

a ○ b = a

b ○ a = b

c ○ a = c

□	a	b	c
a	c	a	a
b	a	c	b
c	a	b	c

○	a	b	c
a	a	a	b
b	b	c	a
c	c	c	b

Arthur Cayley 1821-1895

- Právník
- Studoval Hamiltonovy kvaterniony
- Profesorem čisté matematiky v Cambridge
- Zabýval se teorií invariantů (pro teorii relativity),

  teorií matic (pro kvantovou mechaniku), teorií grup

Příklady binárních operací

- Obyčejné sčítání, násobení, odečítání – binární operace na množině Z všech celých čísel nebo na množině Q všech racionálních čísel nebo na množině R, na množině C všech komplexních čísel
- Dělení není binární operací na žádné z těchto množin (není definováno dělení nulou).
- Odečítání není binární operací na množině N všech přirozených čísel. (Nemůžeme odečítat větší číslo od menšího.)

Vlastnosti binárních operací

- Asociativita operace – při skládání operace nezáleží na uzávorkování

$$(a + b) + c = a + (b + c)$$

- Komutativita – nezáleží na pořadí prvků
- Existence neutrálního prvku
- Existence inverzního prvku ke každému prvku základní množiny

Vlastnosti binárních operací na množině A

- V1 – Asociativita

$\forall\ a,b,c \in A \quad a(bc) = (ab)c$ (multiplikativní zápis)

- V2 – Komutativita

$\forall\ a,b \in A \quad ba = ab$

- V3 – Existence neutrálního (jednotkového) prvku

$\exists\ e \in A \ \ \forall\ a \in A \quad ea = ae = a$

- V4 – Existence inverzního prvku

$\forall\ a \in A \ \ \exists\ a^{-1} \in A \quad aa^{-1} = a^{-1}a = e$

Uzavřenost množiny vzhledem k operaci

- Definice:

  Nechť A je množina s binární operací $*$.

  Podmnožina B množiny A

  je uzavřená vzhledem k operaci $*$,

  jestliže pro každé dva prvky $x, y \in B$ je i $x*y \in B$.
- Příklady: Uvažujme množinu N všech přirozených čísel.
- 1. Podmnožina všech sudých čísel je uzavřená vzhledem k operaci sčítání.
- 2. Podmnožina všech lichých čísel vzhledem ke sčítání uzavřená není (součet dvou lichých čísel je číslo sudé).

Uzavřenost množiny vzhledem k operaci

Příklady:

- N s operací násobení

{1}, podmnožina všech sudých čísel, podmnožina všech lichých čísel, podmnožina všech násobků nějakého přirozeného čísla (Ano)

Podmnožina všech prvočísel (Ne)

- N s operací sčítání

Podmnožina všech čísel dělitelných třemi (Ano)

Algebraické struktury s jednou operací

- Grupoid – množina s jednou binární operací
- Pologrupa (semigroup) – množina s jednou asociativní binární operací
- Monoid – pologrupa, v níž existuje neutrální prvek
- Grupa (group) – množina s jednou asociativní binární operací, v níž existuje neutrální prvek a ke každému prvku existuje prvek inverzní.
  - Abelova grupa (Abelian group) – grupa, v níž je operace navíc komutativní
  - Cyklická grupa (cyclic group)

Definice grupy

G1 – Výsledek operace • libovolných dvou prvků množiny *M* zůstane vždy v množině *M*. (*M* je uzavřená vzhledem k operaci •.)

G2 - Pro každé tři prvky množiny *M* platí asociativní zákon. Prvky *a*, *b*, *c*, nemusí být navzájem různé.

$$a \bullet (b \bullet c) = (a \bullet b) \bullet c$$

G3 – V množině *M* existuje *e* – neutrální prvek tak, že pro všechny prvky *a* z *M* je

$$e \bullet a = a \quad \text{a} \quad a \bullet e = a$$

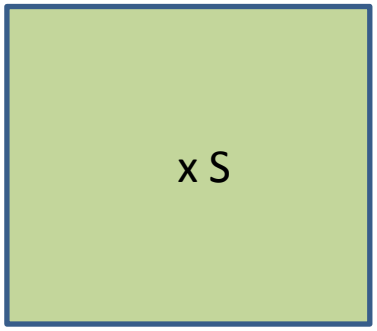
G4 – Ke každému prvku *a* z množiny *M* existuje právě jeden inverzní prvek $a^{-1} \bullet a = a \bullet a^{-1} = e$

Příklad – otáčení čtverce kolem středu

- Nechť je dán čtverec ABCD. Uvažujme množinu R všech takových otočení čtverce ABCD kolem středu S, která převádějí čtverec ABCD opět na tento čtverec – zákrytová otočení čtverce ABCD.
- Dohoda: otočení, která se liší o celočíselný násobek 360° považujeme za stejná
- Množina R se skládá z otočení o úhly O°, 90°, 180° a 270° - a_0, a_1, a_2, a_3
- Otočení o 0° nazýváme identické otočení – identita.

Příklad - otáčení čtverce kolem středu

- Otočení si označíme postupně a_0, a_1, a_2, a_3.
- Např. $a_1 . a_2 = a_3$



A

- Dvě otočení postupně za sebou zapíšeme $a_j . a_i$

(multiplikativní zápis)

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

Příklad – otáčení čtverce kolem středu

Prověříme vlastnosti grupy z definice

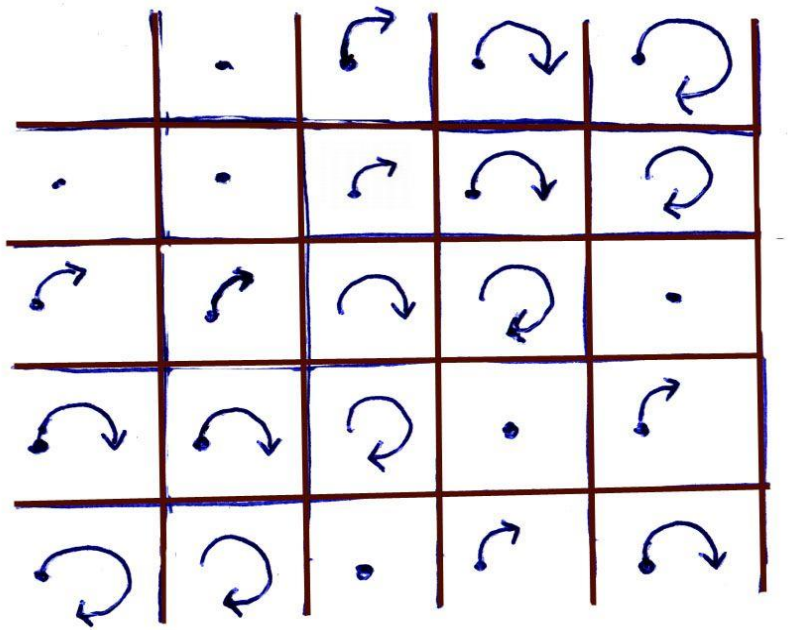
- 1. Uzavřenost množiny
- 2. Asociativita operace
- 3. Existence neutrálního prvku
- 4. Ke každému a_i existuje inverzní prvek.

Otáčení čtverce tvoří grupu, dokonce Abelovu, protože

operace je komutativní.

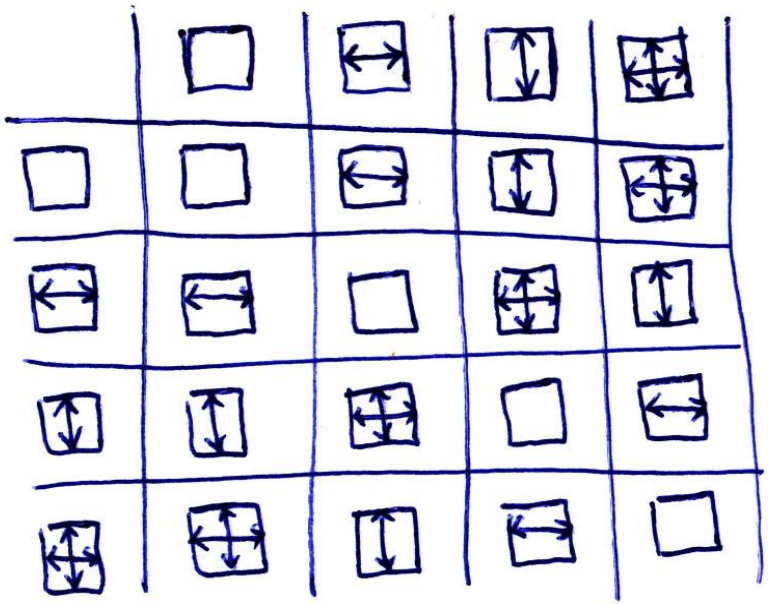
Otáčení versus překlápění

- Otáčení čtverce o 90°



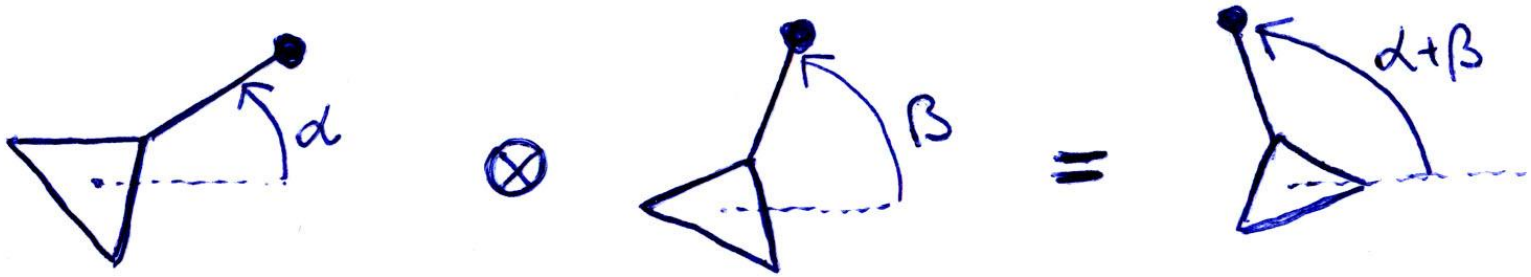
- Cyklická grupa Z_4

- Překlápění čtverce



- Kleinova 4-grupa

Otáčení o daný úhel – nekonečná grupa



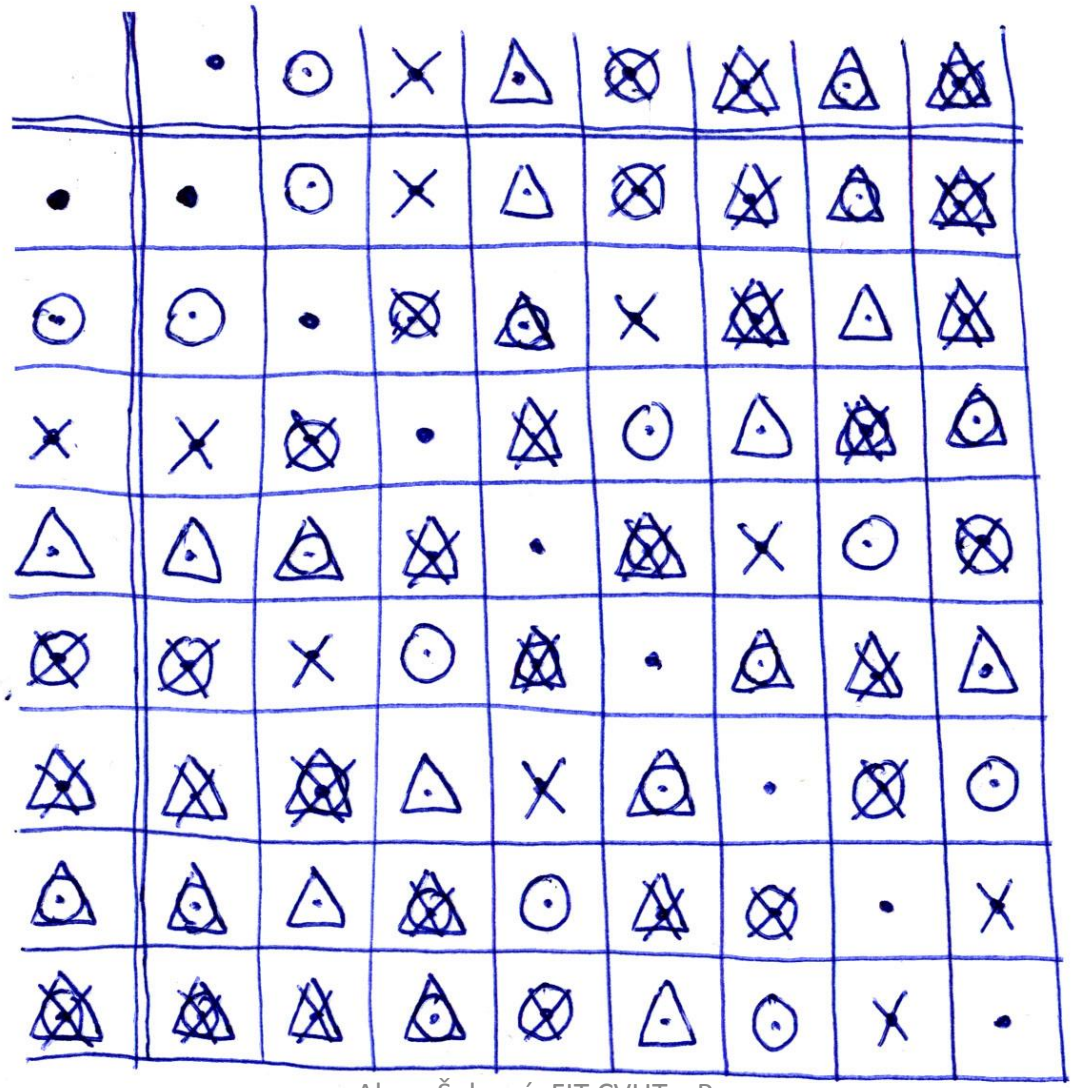
Každému úhlu $\alpha \in \langle 0, 2\pi)$ odpovídá prvek grupy – otočení obrazce o úhel α.

Grupu lze jednoznačně převést na grupu násobení matic rotace:

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \otimes \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}$$

Příklad grupy vyššího řádu



Další příklady grup

- Hodinová grupa (cyklická) – sčítání hodin na ciferníku
- Kulová grupa (grupa transformací, symetrií) – všechna pootočení koule
- Vojenská grupa (cyklická grupa řádu 4) – čtyři povely: vlevo vbok, vpravo vbok, čelem vzad, stůj
- Pochodová grupa – množina všech konečných posloupností povelů vojenské grupy + krok vpřed (včetně prázdné posloupnosti) – sčítání vektorů v Gaussově rovině
- Škatulata, škatulata, hejbejte se – permutační grupa

Příklady grup

- reálná čísla + sčítání
- celá čísla + sčítání
- přirozená čísla + sčítání - **NE!**
- celá čísla + odčítání
- reálná čísla + násobení - **NE!**
- racionální + sčítání
- racionální bez nuly + násobení
- vektory + skládání
- osmiúhelník + překlápění podle os symetrie a rotační symetrie

Podstruktury (Substructures)

- Každá struktura může mít svou podstrukturu.

Podgrupa (Subgroup)

- Nechť G je grupa. Podgrupou grupy G rozumíme libovolnou podpologrupu H grupy G, takovou, že $a^{-1} \in H$ pro každou $a \in H$.

Normální podgrupa (Normal subgroup)

- Podgrupa H se nazývá normální, jestliže $bHb^{-1} \subseteq H$ pro každé $b \in G$.

Normální podgrupy a generátory

- Průnik libovolného systému (normálních) podgrup grupy G je opět (normální) podgrupa grupy G.
- Jestliže $M \subseteq G$, pak průnik všech (normálních) podgrup grupy G obsahujících množinu M se nazývá (normální) podgrupa grupy G generovaná množinou M.
- M se nazývá množinou generátorů této podgrupy.
- Jestliže podgrupa generovaná množinou M je rovna grupě G, pak M se nazývá množinou generátorů grupy G.

Cyklická a konečně generovaná grupa

- Grupa, v níž existuje jednoprvková množina generátorů, se nazývá cyklická (cyclic group).

- Grupa, v níž existuje konečná množina generátorů, se nazývá konečně generovaná (finitely generated group).

Symetrická grupa permutací

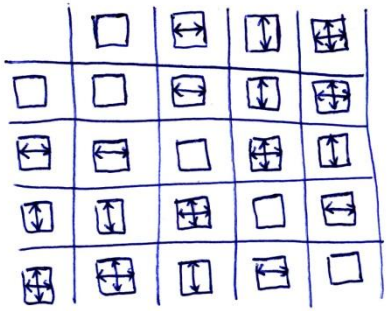
- Nechť M je neprázdná množina. Všechny permutace (bijektivní neboli vzájemně jednoznačné zobrazení) množiny M (na sebe) tvoří grupu vzhledem k operaci skládání.
- Tato grupa se nazývá symetrická grupa S(M) (symmetric group).
- V případě, že množina $M = \{1, 2, \ldots, n\}$, budeme ji značit S_n .
- Vyšetřete, zda platí: Grupa S(M) je komutativní, právě když počet prvků množiny je větší než 2.

Příklady

- Rombická grupa

  K = { (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)}

- K – Kleinova čtyřgrupa (Klein four – group)



- nejmenší necyklická grupa
- isomorfní s grupou symetrií obdélníku i kosočtverce

- Felix Klein, 1884 (Vierergruppe)
- $a^2=b^2=c^2=e$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$

Axiomatická teorie grup a její vlastnosti

Soustava axiomů může mít dvě důležité vlastnosti:

- Bezespornost – nemožnost dokázat z tohoto systému dokázat dvě tvrzení, která by si vzájemně odporovala
- Úplnost – Systém axiomů je úplný, když o pravdivosti libovolného tvrzení o pojmech vyšetřovaných v této teorii lze rozhodnout na základě tohoto systému axiomů
- Poznámka: Požadavek úplnosti není nezbytně nutný. Existuje řada teorií, které úplné nejsou (např. většina algebraických teorií).

  Zato požadavek bezespornosti je nutný vždy.

Axiomy teorie grup

G1 – Výsledek operace • libovolných dvou prvků množiny *M* zůstane vždy v množině *M*. (*M* je uzavřená vzhledem k operaci •.)

G2 - Pro každé tři prvky množiny *M* platí asociativní zákon. Prvky *a*, *b*, *c*, nemusí být navzájem různé.

$$a \bullet (b \bullet c) = (a \bullet b) \bullet c$$

G3 – V množině *M* existuje *e* – neutrální prvek tak, že pro všechny prvky *a* z *M* je

$$e \bullet a = a \quad \text{a} \quad a \bullet e = a$$

G4 – Ke každému prvku *a* z množiny *M* existuje právě jeden inverzní prvek $a^{-1} \bullet a = a \bullet a^{-1} = e$

Co předcházelo vzniku teorie grup?

- Rozvoj teorie čísel na konci 18. století
- Rozvoj teorie algebraických rovnic na konci 18. století vedoucí ke studiu permutací
- Rozvoj geometrie na počátku 19. století

Počátky teorie grup

- Jsou spojeny s teorií algebraických rovnic, tj.

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

Metody užívali Joseph L. Lagrange (1771)

Paolo Ruffini (1799)

Niels H. Abel (1824)

Evariste Galois (1830)

Vlastnosti rovnice a Galoisovy grupy jsou na sobě závislé.

Jiný zdroj vzniku teorie grup

Druhá polovina 19. století

- Felix Klein
- Erlangenský program – 1872

Každé geometrii
odpovídá grupa transformací
a
pomocí těchto grup lze utřídit
dosud známé geometrické teorie.

Aplikace

- Grupy např. umožňují charakterizovat symetričnost geometrických obrazců a těles, a to pomocí jejich zákrytových pohybů – využití v krystalografii – klasifikace pravidelných prostorových systémů
- Kvantová mechanika – reprezentace grup pomocí lineárních zobrazení

Lámejte si hlavu - L1

- Určete všechny podgrupy v grupě zadané Cayleyho tabulkou:

	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y