GRUPY: STRUčNý ÚVOD V KONTEXTU LINEÁRNÍ ALGEBRY

DAVID STANOVSKÝ

Cílem tohoto textu je seznámit posluchače kurzu lineární algebry s pojmem grupy a uvést základní příklady grup, které vychází z objektů studovaných v lineární algebře: především tedy grupy permutací a grupy matic. Číslované odkazy vedou na definice a tvrzení ve skriptech Barto-Tůma.

0.1. **Grupy.** Hlavní motivací teorie grup je studium nejrůznějších typů symetrií a transformací matematických objektů. Pojem pochází z Galoisovy teorie a původně označoval množinu G (tj. skupinu, grupu) zobrazení na množině X uzavřenou na skládání, tj. splňující $\pi \circ \sigma \in G$ pro všechna $\pi, \sigma \in G$. Abstrakcí tohoto pojmu vznikla rozsáhlá větev algebry, zvaná teorie grup. Aplikace nachází všude, kde se vyskytuje pojem symetrie či transformace.

Definice. *Grupou* rozumíme množinu G, na které jsou definovány binární operace $*$, unární operace $'$ a konstanta $e \in G$ splňující pro každé $a, b, c \in G$ následující podmínky:

$$a * (b * c) = (a * b) * c, \qquad a * e = e * a = a, \qquad a * a' = a' * a = e.$$

Grupu nazýváme *abelovskou*, pokud navíc pro všechna $a, b \in G$ platí

$$a * b = b * a.$$

Prvku e se říká *jednotka*, prvku a' *inverzní prvek* k prvku a. Grupu formálně zapisujeme jako čtveřici $\mathbf{G} = (G, *, ', e)$.

V konkrétních příkladech bývá typickou trojicí operací buď $+, -, 0$, pak hovoříme o *aditivním zápise* (a místo $x + (-y)$ píšeme $x - y$), anebo trojice $\cdot, ^{-1}, 1$, čemuž říkáme *multiplikativní zápis*.

Projděte si celou přednášku z lineární algebry a hledejte grupy!

Hned v kapitole 1 se v principu pracuje s dvěma dobře známými grupami.

Příklad. Reálná čísla s operací sčítání tvoří grupu, $(\mathbb{R}, +, -, 0)$. Obecněji, reálné aritmetické vektory s n složkami s operací sčítání tvoří grupu, $(\mathbb{R}^n, +, -, \mathbf{0})$. Nenulová reálná čísla s operací násobení tvoří grupu, $(\mathbb{R} \setminus \{0\}, \cdot, ^{-1}, 1)$. Grupové axiomy jsou očividně splněny.

Všimněte si, že tělesa jsou definovány pomocí dvou grupových operací navzájem svázaných distributivním zákonem. Definici tělesa můžeme přeformulovat takto: množina T s operacemi $+, -, \cdot, ^{-1}$ a prvky $0 \neq 1$ se nazývá těleso, pokud $(T, +, -, 0)$ je abelovská grupa, $(T \setminus \{0\}, \cdot, ^{-1}, 1)$ je abelovská grupa a platí $a(b+c) = ab + ac$ pro všechna $a, b, c \in T$. V opačném směru, s každým tělesem máme spojeny dvě grupy:

Příklad (aditivní a multiplikativní grupa tělesa)**.** Buď T těleso. Pak

- $(T, +, -, 0)$ je abelovská grupa, tzv. *aditivní grupa* tělesa T,
- $\mathbf{T}^* = (T \setminus \{0\}, \cdot, ^{-1}, 1)$ je abelovská grupa, tzv. *multiplikativní grupa* tělesa T.

Grupové axiomy jsou obsaženy v definici tělesa.

Místo těles lze brát i obecnější struktury, tzv. okruhy, se kterými se seznámíte v kurzu obecné algebry. Mezi odvozenými grupami zmiňme tzv. *cyklické grupy*.

Date: 29. května 2020.

Příklad. Celá čísla tvoří grupu $\mathbb{Z} = (\mathbb{Z}, +, -, 0)$. Čísla v intervalu $0, ..., n-1$ tvoří grupu $\mathbb{Z}_n = (\{0, ..., n-1\}, +, -, 0)$, kde sčítání i odčítání bereme modulo n.

Podobně, definice vektorového prostoru říká, že $(V, +, -, 0)$ je abelovská grupa a dále je definováno násobení skalárem splňující jistá pravidla (související s grupou automorfismů aditivní grupy, ale tenhle pohled si necháme do kurzu obecné algebry).

V kapitole 4 se definuje sčítání a násobení matic. Matice $n \times n$ nad tělesem T tvoří grupu vzhledem ke sčítání, ale nikoliv vzhledem k násobení, protože ne každá matice má matici inverzní. Nicméně, pokud se omezíme na regulární matice, grupu vzhledem k násobení dostaneme: Tvrzení 4.87 říká, že součin regulárních matic je regulární a Tvrzení 4.34 říká, že násobení matic je asociativní. Jde o jeden z nejdůležitějších příkladů grup.

Příklad (obecná lineární grupa)**.** Buď T těleso. Pak

$$\mathbf{GL}_n(T) = (\{A : \ A \text{ je regulární matice } n \times n \text{ nad tělesem } T\}, \cdot, ^{-1}, I_n)$$

je grupa, tzv. *obecná lineární grupa* nad tělesem T stupně n.

Skládání zobrazení je asociativní, ale ne každé zobrazení má inverz. Bijektivní zobrazení na dané množině X (neboli permutace na X) ovšem grupu tvoří, jednotkou bude identické zobrazení id. Jde o druhý z nejdůležitějších příkladů grup.

Příklad (symetrická grupa)**.** Buď X množina. Pak

$$\mathbf{S}_X = (\{\pi : \ \pi \text{ je permutace na množině } X\}, \circ, ^{-1}, id).$$

je grupa, tzv. *symetrická grupa* na množině X. Je-li $X = \{1, \ldots, n\}$, pak místo $\mathbf{S}_X$ píšeme $\mathbf{S}_n$.

Podobně, lineární operátory na vektorovém prostoru V grupu netvoří (inverzy!), ale ty z nich, které jsou bijektivní, ano. Hovoříme o obecné lineární grupě na prostoru V,

$$\mathbf{GL}(V) = \{f : \ f : V \to V \text{ bijektivní lineární zobrazení }\}, \circ, ^{-1}, id).$$

V definici jsou skryta Tvrzení 6.15 a 6.16, která říkají, že složení lineárních zobrazení jsou lineární, a inverz bijektivní lineárního zobrazení je také lineární. Pro aritmetické prostory jsou prvky $\mathbf{GL}(T^n)$ a $\mathbf{GL}_n(T)$ ve vzájemně jednoznačné korespondenci, a to dokonce tak, že skládání zobrazení odpovídá násobení příslušných matic (viz kapitola 6). Takovým korespondencím se říká *izomorfismy* a detailně se s nimi seznámíme v kurzu obecné algebry.

0.2. **Podgrupy.** Poslední příklad nás navádí na pojem *podgrupy*, jakési analogie pojmu podprostor v kontextu grup. Bijektivní lineární operátory na V jsou vlastně permutace na množině V, jde tedy o jakousi část grupy S_V, dokonce používáme stejné operace skládání a invertování zobrazení (formálně vzato, jde o restrikci operace skládání na podmnožinu lineárních operátorů).

Definice. Buď $\mathbf{G} = (G, *, ', e)$ grupa a $H \subseteq G$ podmnožina její nosné množiny taková, že

- $e \in H$,
- pro každé $a \in H$ platí $a' \in H$,
- pro každé $a, b \in H$ platí $a * b \in H$.

Říkáme, že H je *uzavřena na grupové operace* a že *tvoří podgrupu* grupy $\mathbf{G}$. Čtveřici $\mathbf{H} = (H, *|_H, '|_H, e)$ pak nazýváme *podgrupou*, přičemž $|_H$ značí restrikci operací na množinu H. Značíme $\mathbf{H} \leq \mathbf{G}$.

Všimněte si, že podgrupa grupy $\mathbf{G}$ je opět grupa: axiomy platné pro všechny prvky G budou jistě splněny i na podmnožině H.

Příklad. Sudá čísla tvoří podgrupu grupy $\mathbb{Z}$:

- 0 je sudá,
- pro každé a sudé platí, že $-a$ je sudé,

- součet sudých čísel je sudý.

Naopak podgrupu netvoří například lichá čísla (0 není lichá), nezáporná čísla (je-li $a > 0$, pak $-a < 0$) ani množina $H = \{a : 2 \mid a \text{ nebo } 3 \mid a\}$, protože například $2 + 3 = 5 \notin H$.

Příklad. Buď V vektorový prostor. Pak $\mathbf{GL}(V)$ je podgrupou $\mathbf{S}_V$, neboť

- id je lineární zobrazení,
- inverz bijektivního lineárního zobrazení je lineární,
- složení lineárních zobrazení je lineární.

Příklad. Sudé permutace tvoří podgrupu grupy $\mathbf{S}_n$, neboť podle Tvrzení 7.11

- id je sudá,
- inverz sudé permutace je sudý,
- složení sudých permutací je sudá permutace.

Tato grupa se nazývá *alternující* a značí se $\mathbf{A}_n$.

Řada maticových pojmů definuje zajimavé podgrupy obecné lineární grupy.

Příklad. Matice s determinantem 1 tvoří podgrupu grupy $\mathbf{GL}_n(T)$, neboť podle Vět 7.26 a 7.27

- $\det I_n = 1$,
- je-li $\det A = 1$, pak $\det A^{-1} = (\det A)^{-1} = 1$,
- je-li $\det A = \det B = 1$, pak $\det AB = \det A \det B = 1$.

Tato grupa se nazývá *speciální lineární grupa* a značí se $\mathbf{SL}_n(T)$.

Příklad. Ortogonální matice tvoří podgrupu grupy $\mathbf{GL}_n(\mathbb{R})$, neboť

- I_n je ortogonální,
- inverz ortogonální matice A je ortogonální matice A^T,
- součin ortogonálních matic je ortogonální (Důsledek 8.85).

Tato grupa se nazývá *ortogonální grupa* a značí se $\mathbf{O}_n$. Analogicky se definují *unitární grupy* $\mathbf{U}_n \leq \mathbf{GL}_n(\mathbb{C})$.

Lemma 0.1. *Průnik podgrup je podgrupa.*

Důkaz. Buď $\mathbf{G} = (G, *, ', e)$ grupa, uvažujme podgrupy $\mathbf{H}_i$, $i \in I$, a označme $H = \bigcap_{i \in I} H_i$. Pak

- $e \in H_i$ pro všechna i, a tedy $e \in \bigcap H_i$,
- pokud $a \in \bigcap H_i$, pak $a \in H_i$ pro všechna i, tedy také $a' \in H_i$ pro všechna i, a tedy $a' \in \bigcap H_i$,
- pokud $a, b \in \bigcap H_i$, pak $a, b \in H_i$ pro všechna i, tedy také $a * b \in H_i$ pro všechna i, a tedy $a * b \in \bigcap H_i$.

□

Příklad. Ortogonální matice s determinantem 1 tvoří podgrupu grupy $\mathbf{GL}_n(\mathbb{R})$, protože jsou průnikem podgrup $\mathbf{SL}_n(\mathbb{R})$ a $\mathbf{O}_n$. Této grupě se říká speciální ortogonální grupa a značí se $\mathbf{SO}_n$. Podle Tvrzení 10.26 lze grupu $\mathbf{SO}_3$ ztotožnit s rotacemi v $\mathbb{R}^3$.

Mezi další zajímavé příklady grup patří například grupy symetrií různých geometrických objektů (čtverec, krychle, ...), jakožto podgrupy grupy všech izometrií, resp. grupy $\mathbf{GL}_n(\mathbb{R})$, pokud jde o n-dimenzionální útvary symetrické kolem počátku. Například grupa symetrií pravidelného n-úhelníka sestává z n rotací (o $k \cdot 2\pi/n$, kde $k = 0, ..., n-1$) a n reflexí (podle os spojujících protilehlé vrcholy, resp. středy hran) a říká se jí *dihedrální grupa*. Studium těchto grup si necháme do kurzu obecné algebry.

Posledním příkladem, který uvedeme, je kvaternionová grupa, která se poněkud vymyká předchozím příkladům.

Příklad. *Kvaternionová grupa* $\mathbf{Q}_8$ je definovaná na množině $\{\pm 1, \pm i, \pm j, \pm k\}$. Násobení je dáno vzorci

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j,$$

a dále pravidly $xy = -(yx)$ a $(-x)y = x(-y) = -(xy)$ pro všechna $x, y \in \{i, j, k\}$.

Pomocí kvaternionové grupy se definuje nekomutativní těleso kvaternionů jako těleso všech výrazů $a+bi+cj+dk$, $a, b, c, d \in \mathbb{R}$. Podobnou konstrukci lze provést v principu pro jakoukoliv grupu, ale těleso kvaternionů se vymyká tím, že jeho multiplikativní grupa úzce souvisí s grupou rotací $\mathbf{SO}_3$. O tom se dočtete více v sekci 3.5.5, jejímž hlavním sdělením je, že rotaci o úhel α kolem osy dané vektorem $(a, b, c)^T$ lze reprezentovat kvaternionem

$$\cos(\alpha/2) + \sin(\alpha/2)(ai + bj + ck),$$

přičemž rotace se skládají tak, jak se příslušné kvaterniony násobí (ejhle, homomorfismus grup). Více se dozvíte v kurzu geometrie v druhém ročníku.

Cvičení.

1. Rozhodněte, zda existuje unární operace $'$ a prvek e tak, aby následující čtveřice byla grupou:

(a) $(\mathbb{Z}, -, ', e)$
(b) $(\mathbb{Q}, *, ', e)$ kde $a * b = |a \cdot b|$.
(c) $(P(X), \cap, ', e)$, kde $P(X)$ značí množinu všech podmnožin množiny X
(d) $(P(X), *, ', e)$, kde $*$ značí symetrickou diferenci, tj. $A * B = (A \cup B) \setminus (A \cap B)$.

[ne, ne, ne, ano]

2. Určete, v kterých z následujících grup tvoří sudá čísla podgrupu: $\mathbb{Z}$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{16}$, $\mathbb{Z}_7^*$. [ano, ne, ano, ne]

3. Ověřte, že $\{z \in \mathbb{C} : \ |z| = 1\}$ tvoří podgrupu grupy $\mathbb{C}^*$. Ověřte, že množina sestávající ze všech kořenů polynomu $x^n - 1$ tvoří podgrupu této grupy.

4. Tvoří matice s kladným determinantem podgrupy grupy $\mathbf{GL}_n(T)$? A co horní, resp. dolní trojúhelníkové matice? A co symetrické, resp. antisymetrické matice? [ano, ano/ano, ne/ne]