GENERÁTORY A HOMOMORFISMY

ALEXANDER „OLIN“ SLÁVIK

1. Vektorové prostory

Nechť $\Bbbk$ je těleso a V, W vektorové prostory nad $\Bbbk$. Jak dobře popsat všechny homomorfismy, tj. $\Bbbk$-lineární zobrazení $f\colon V \to W$?

Můžeme si vzít vhodnou podmnožinu $M \subseteq V$, která už celý prostor V nageneruje a popsat, kam f zobrazí prvky M; jsou-li totiž f a g dva homomorfismy, které se shodují na M, pak už se musí shodovat na celém V. Je-li totiž $v \in V$ libovolný, pak lze zapsat jako $v = a_1w_1 + \cdots + a_nw_n$, kde $a_i \in \Bbbk$ a $w_i \in M$, takže

$$f(v) = a_1f(w_1) + \cdots + a_nf(w_n) = a_1g(w_1) + \cdots + a_ng(w_n) = g(v).$$

Množina M může být zvolena i hodně „hloupě“, v extrémním případě to může být i celý prostor V; nemůžeme tedy zobrazovat prvky M na úplně libovolné prvky W a myslet si, že dostaneme homomorfismus. Pokud např. vezmeme $V = \Bbbk^2$, $M = \{(1,0)^T, (0,1)^T, (1,1)^T\}$, pak každý homomorfismus f z V kamkoliv musí samozřejmě splňovat

$$f((1,1)^T) = f((1,0)^T) + f((0,1)^T).$$

Toto je všechno samozřejmé a znalec lineární algebry namítne, proč se zde zabýváme takovými banalitami, když si za M můžeme vzít *bázi* V, její prvky posílat „úplně kamkoliv“ a vždy získat jednoznačně daný homomorfismus. Vskutku tomu tak bude, ale než půjdeme dále, podívejme se na následující dvě ekvivalentní definice báze vektorového prostoru [1, Tvrzení 5.56]:

(1) lineárně nezávislá množina generátorů,
(2) minimální množina generátorů.

V jistém smyslu se možná dá říct, že ekvivalence těchto dvou definicí je důvodem, *proč je lineární algebra tak jednoduchá*. V dalších sekcích typicky analogie (1) vůbec nebude existovat, analogii k (2) mít často k dispozici budeme, ale rozhodně to nebude zdaleka tak silný nástroj, jako je báze vektorových prostorů.

2. Grupy

Nechť $\mathbf{G}$, $\mathbf{H}$ jsou grupy a opět se zabývejme otázkou popisu (grupových) homomorfismů $f\colon \mathbf{G} \to \mathbf{H}$. Stejně jako u vektorových prostorů, i nyní si můžeme vzít nějakou množinu generátorů $\mathbf{G}$ a posílat její prvky „někam“ do $\mathbf{H}$, čímž už bude homomorfismus jednoznačně popsán – pokud onou volbou vůbec homomorfismus dostaneme, přesněji řečeno zda ona funkce, nijak nerespektující grupovou strukturu, půjde rozšířit do grupového homomorfismu.

Asi hned narazíme na problém, že „grupy nemají báze“. Pro nekonečné grupy se nám může velmi snadno stát, že nenajdeme ani žádnou množinu generátorů, která by byla minimální co do inkluze – jedním takovým příkladem je aditivní grupa $\mathbb{Q}$. *Konečné* grupy samozřejmě minimální množiny generátorů mají (nemůžeme „vyhazovat prvky donekonečna“), ale ty zase typicky nebudou „nezávislé“ – budou mezi nimi nějaké vztahy neboli *relace*.

Co to znamená? Ve výše uvedeném příkladu vektorového prostoru $\Bbbk^2$ a jeho zbytečně velké množiny generátorů M jsme měli evidentní vztah $(1,1)^T = (1,0)^T + (0,1)^T$, který musely – kvůli homomorfnosti – splňovat i libovolné obrazy těchto tří vektorů. Nechť je nyní $\mathbf{G}$ cyklická n-prvková grupa[1] s generátorem g a jednotkovým prvkem $1_{\mathbf{G}}$. Už samotná tato jednoprvková

[1] Neboli $\mathbb{Z}_n$, ale bude se mi víc hodit zapisovat grupovou operaci vždy multiplikativně, ať v tom není ještě větší nepořádek.

množina $\{g\}$, byť evidentně minimální, není „nezávislá“, protože platí $g^n = 1_{\mathbf{G}}$, a je-li $f\colon \mathbf{G} \to \mathbf{H}$ homomorfismus, pak musí platit

$$f(g)^n = 1_{\mathbf{H}}.$$

Není těžké nahlédnout, že bude-li prvek $f(g)$ splňovat tuto podmínku, máme už jednoznačně zadaný grupový homomorfismus $f\colon \mathbf{G} \to \mathbf{H}$.

Pokročme o úroveň dál a vezměme si např. grupu $\mathbf{S}_3$, která je generována např. permutacemi $\pi = (1\,2)$ a $\varrho = (1\,3)$. Prvky π a ϱ mají oba řád 2, takže je-li $f\colon \mathbf{G} \to \mathbf{H}$ homomorfismus, musí platit $f(\pi)^2 = 1_{\mathbf{H}}$ a $f(\varrho)^2 = 1_{\mathbf{H}}$. To ale není všechno! Kdyby bylo, mohli bychom mít třeba grupový homomorfismus $f\colon \mathbf{S}_3 \to \mathbb{Z}_2 \times \mathbb{Z}_2$, který by splňoval $f(\pi) = (1,0)$ a $f(\varrho) = (0,1)$ (což zřejmě splňuje výše uvedenou řádovou podmínku). Máme ovšem $\pi\varrho = (1\,3\,2)$ a $\varrho\pi = (1\,2\,3)$, takže

$$f((1\,3\,2)) = f(\pi\varrho) = f(\pi) + f(\varrho) = (1,1) = f(\varrho) + f(\pi) = f(\varrho\pi) = f((1\,2\,3)).$$

Je ovšem $(1\,3\,2) = (1\,2\,3)^2$, přičemž aplikace f na tuto rovnost dá

$$(1,1) = f((1\,3\,2)) = f((1\,2\,3)^2) = 2 \cdot f((1\,2\,3)) = 2 \cdot (1,1) = (0,0),$$

spor.

Je tedy nutné vzít v úvahu i *relace generátorů mezi sebou*, což jsme úplně samozřejmě udělali i v našem jednoduchém příkladu s vektorovými prostory. Narážíme ale na problém: které relace tedy vzít v úvahu? Vždyť v $M \subseteq \mathbb{k}^2$ kromě oné skloňované

$$(\star) \qquad (1,1)^T = (1,0)^T + (0,1)^T$$

můžeme vymyslet i jiné relace, např.

$$2 \cdot (1,0)^T - (1,1)^T = (1,1)^T - 2 \cdot (0,1)^T$$

a spoustu jiných podobných, které každý homomorfismus vektorových prostorů musí respektovat. Lze ovšem nahlédnout, že *všechny* relace mezi prvky M už plynou z $(\star)$, a to *pouze aplikací axiomů vektorových prostorů*. Tím pádem stačí pro existenci homomorfismu ověřit platnost $(\star)$ pro obrazy prvků M.

Zpátky ještě k příkladu s cyklickou grupou řádu n: kromě relace

$$(\spadesuit) \qquad g^n = 1_{\mathbf{G}}$$

máme třeba taky $g^{777n} = 1_{\mathbf{G}}$ nebo třeba $g^{777n+1} = g$; tyto nám ale nedávají žádnou novou informaci – *jakýkoliv* prvek *jakékoliv* grupy splňující $(\spadesuit)$ splňuje už i tyto další „redundantní“ relace. Jinak řečeno, tyto další relace *lze z* $(\spadesuit)$ *vyvodit čistě aplikací axiomů grup*.

Co se týče $\mathbf{S}_3$, ukazuje se, že kromě relací $\pi^2 = \mathrm{id}$, $\varrho^2 = \mathrm{id}$ potřebujeme ještě tyto dva prvky svázat vztahem

$$(\diamondsuit) \qquad \pi\varrho\pi = \varrho\pi\varrho$$

(obě strany se rovnají transpozici $(2\,3)$) a máme vyhráno – z této relace už plynou všechny ostatní. Jinak řečeno, je-li $\mathbf{H}$ libovolná grupa, pak všechny grupové homomorfismy $f\colon \mathbf{S}_3 \to \mathbf{H}$ jsou popsány volbou prvků $f(\pi), f(\varrho) \in H$ splňujících

$$f(\pi)^2 = 1_{\mathbf{H}}, \quad f(\varrho)^2 = 1_{\mathbf{H}} \quad \text{a} \quad f(\pi)f(\varrho)f(\pi) = f(\varrho)f(\pi)f(\varrho).$$

Pokud budeme chtít např. popsat homomorfismy $\mathbf{S}_3 \to \mathbb{Z}_2 \times \mathbb{Z}_2$, pak si všimneme, že rovnici $(\diamondsuit)$ v $\mathbb{Z}_2 \times \mathbb{Z}_2$ a vůbec každé komutativní grupě můžeme splnit jenom tak, že se budou ony dva prvky rovnat. Podmínky na řády prvků budou určitě splněny, takže následující tabulka uvádí *všechny* homomorfismy $\mathbf{S}_3 \to \mathbb{Z}_2 \times \mathbb{Z}_2$:

$f(\pi)$	$f(\varrho)$
$(0,0)$	$(0,0)$
$(1,0)$	$(1,0)$
$(0,1)$	$(0,1)$
$(1,1)$	$(1,1)$

Toto je sice pěkné, ale vkrádají se přirozené otázky: *Proč* $(\diamondsuit)$ *opravdu stačí? Jak se přijde na takovéto relace u jiných grup?* Že podobná sada relací bude stačit pro libovolnou symetrickou

grupu se lze přesvědčit např. zde. Odpověď na druhou otázku zní „těžko“. Jde v podstatě o hledání tzv. *prezentace grupy*, což je asi obecně algoritmicky celkem obtížná procedura. Na oné wikistránce můžete nalézt příklady prezentací pro spousty různých grup.[2]

Možná ještě někoho může napadnout, zda přece jen neexistují nějaké grupy, které by „měly bázi“, tj. množinu generátorů, jejíž prvky by nesplňovaly „žádné“ relace, přesněji řečeno jen ty relace, které lze vyvodit pomocí axiomů teorie grup „z ničeho“. Takové grupy vskutku existují a říká se jim *volné grupy*. Např. volná grupa s jedním generátorem je isomorfní grupě $\mathbb{Z}$, což mimo jiné znamená přesně to, že homomorfismy ze $\mathbb{Z}$ do *libovolné* grupy jsou zadány tím, kam pošleme generátor $1 \in \mathbb{Z}$, který můžeme poslat *kamkoliv* – stejně jako prvky báze vektorového prostoru. Z tohoto pohledu je lineární algebra o tolik jednodušší než teorie grup, protože každý vektorový prostor je „volný“; bližší podrobnosti viz teorie kategorií a univerzální algebra :-)

3. Tělesa a Galoisovy grupy

Nechť $\Bbbk$ je těleso a f polynom s koeficienty $\Bbbk$. Nechť $a_1, \ldots, a_n$ jsou všechny kořeny f, takže $\mathbb{K} = \Bbbk(a_1, \ldots, a_n)$ je přesně rozkladové nadtěleso polynomu f. To je nejmenší nadtěleso a dokonce nadokruh $\Bbbk$, který obsahuje prvky $a_1, \ldots, a_n$ – každý prvek $\mathbb{K}$ je polynom v $a_1, \ldots, a_n$ s koeficienty v $\Bbbk$. Z toho tedy plyne, že libovolný tělesový $\Bbbk$-homomorfismus $\varphi\colon \mathbb{K} \to \mathbb{L}$ je jednoznačně zadán svými hodnotami na $a_1, \ldots, a_n$, které tak můžeme chápat jako *generátory* $\mathbb{K}$ nad $\Bbbk$.

Stejně jako v případě vektorových prostorů a grup, i zde narážíme na problém, že ony generátory nemusí být *nezávislé*, tj. mohou mezi nimi být nějaké *relace*. První takovou relací, které si lze všimnout, je skutečnost, že $f(a_i) = 0$, takže musí platit i $f(\varphi(a_i)) = 0$ (φ nechává prvky $\Bbbk$ na místě, takže koeficienty v polynomu f se nezmění) – pokud se tedy bavíme o Galoisových grupách a $\Bbbk$-isomorfismech $\mathbb{K} \to \mathbb{K}$, pak *tyto $\Bbbk$-isomorfismy jsou vlastně jen permutace kořenů f*.

Další typ relací, který vždy máme, jsou Vietovy vztahy, které musí kořeny splňovat mezi sebou. Protože tyto vztahy jsou vyjádřeny *symetrickými* polynomy (dokonce těmi elementárními!), nedávají nám žádné omezení na to, které permutace kořenů f jsou „přípustné“ a které ne.

Bohužel tyto „samozřejmé“ relace mohou, ale nemusí být všechno, což je důvod, proč na výpočet Galoisových grup (polynomů libovolných stupňů) není žádná přímočará „kuchařka“. Máme-li např. polynom $f = x^3 - 2 \in \mathbb{Q}[x]$, pak dle výpočtů z přednášky je jeho Galoisova grupa nad $\mathbb{Q}$ isomorfní $\mathbf{S}_3$, tedy jeho kořeny a_1, a_2, a_3 mezi sebou nesplňují žádné relace, *které by nešly vyvodit z výše uvedených relací pomocí axiomů tělesových rozšíření* $\mathbb{Q}$, tj. pouze „samozřejmé relace“ jako třeba

$$a_1^2 a_2 a_3 + 10 = -2a_1 + 10$$

(plyne z Vietova vztahu pro absolutní člen) nebo

$$a_2^3 = a_3^3$$

(plyne z toho, že to jsou kořeny $x^3 - 2$).

Oproti tomu rovněž na přednášce diskutovaný $g = x^3 - \frac{3}{4}x - \frac{1}{8} \in \mathbb{Q}[x]$ je komplikovaný v tom, že jeho kořeny a_1, a_2, a_3, tj. generátory $\mathbb{Q}(a_1, a_2, a_3)$ splňují ještě další relace, konkrétně (při vhodném uspořádání)

$$\begin{aligned} a_2 &= 64a_1^7 - 112a_1^5 + 56a_1^3 - 7a_1, \\ a_3 &= 64a_2^7 - 112a_2^5 + 56a_2^3 - 7a_2, \\ a_1 &= 64a_3^7 - 112a_3^5 + 56a_3^3 - 7a_3 \end{aligned}$$

[2] To, že prezentace grup se obecně špatně hledají, ovšem ještě neznamená, že popis všech homomorfismů mezi nějakými grupami je beznadějný úkol! Např. v tomto konkrétním příkladu vidíme, že všechny trojcykly v $\mathbf{S}_3$ se musí poslat na $(0,0)$ (protože $\mathbb{Z}_2 \times \mathbb{Z}_2$ nemá prvky řádu 3) a protože se každé dvě transpozice v $\mathbf{S}_3$ liší o trojcyklus, musíme všechny transpozice poslat na tentýž prvek $\mathbb{Z}_2 \times \mathbb{Z}_2$. Alternativně můžeme říct, že trojcykly, které se pošlou na $(0,0)$, tvoří normální podgrupu, faktor podle které je isomorfní $\mathbb{Z}_2$.

(to je onen Čebyševův polynom), ale třeba

$$a_1 \neq 64a_2^7 - 112a_2^5 + 56a_2^3 - 7a_2,$$

takže můžeme kořeny jen „cyklit“, nikoliv libovolně permutovat. Protože víme, že příslušná Galoisova grupa musí být tříprvková cyklická, veškeré další relace mezi a_1, a_2, a_3 už musí jít vyvodit z výše uvedených rovností pomocí axiomů tělesových rozšíření $\mathbb{Q}$.

Mimochodem, na Wikipedii se lze dočíst[3], že Galoisova teorie vskutku původně začínala jako studium permutací kořenů $a_1, \ldots, a_n$ takových, že pokud sada $(a_1, \ldots, a_k)$ splňuje nějakou algebraickou rovnici s koeficienty v $\Bbbk$, pak musí tutéž rovnici splňovat i zpermutovaná sada $(\varphi(a_1), \ldots, \varphi(a_n))$.

Reference

[1] Libor Barto a Jiří Tůma, *Lineární algebra* (skripta), www.karlin.mff.cuni.cz/~stanovsk/vyuka/skripta_la6.pdf

[3] A přijde mi, že to fakt stojí za přečtení, jsou tam i hezké příklady.