3. kapitola. Obecný pojem grupy. Jiné příklady grup

In: Ladislav Rieger (author): O grupách. (Czech). Praha: Mladá fronta, 1974. pp. 21–42.

Persistent URL: http://dml.cz/dmlcz/403814

3. kapitola

OBECNÝ POJEM GRUPY. JINÉ PŘÍKLADY GRUPY

K vytčení čtyř axiomů grupy jsme byli přivedeni potřebou objasnit pojem geometrické pravidelnosti; při tom se ukázalo, že axiomy grupy, platící pro skládání zákrytových pohybů geometricky pravidelného útvaru jsou vlastně některými početními zákony, které platí pro násobení čísel (např. kladných zlomků). Avšak ukážeme si, v jak rozmanitých dalších podobách nalézáme splněny tytéž axiomy grupy (1) až (4) z 2. kap. K tomu si výslovně uvědomme následující. Axiomy grupy budou splněny vždy nějakým násobení připomínajícím úkonem, např. „skládáním" (pohybů) prováděným s předměty, kterým budeme od nynějška říkat *prvky grupy*. Množina všech těchto prvků musí s libovolnými dvěma svými prvky obsahovat i výsledek „násobení" („složení") na ně v daném pořadí provedeného. Množinu s takovýmto „násobením", pro niž jsou splněny axiomy grupy, nazýváme *grupou vzhledem* k uvedenému *„násobení"*. Chceme-li tedy výslovně formulovat axiomy grupy obecně, vrátíme se do předchozí 2. kapitoly a slova „zákrytový pohyb" nahradíme slovy „prvek grupy", slova „zpětný pohyb", slovy „inversní prvek", slova „identický pohyb" slovy „jednotkový prvek", nebo i stručněji „jednotka", a konečně slova „skládání pohybů" slovem „násobení". Musíme však mít stále na paměti, *že slovo jednotka a slovo násobení* (přesněji řečeno: jednotka grupy a grupové násobení) *a odpovídající názvy, jako součin,*

mocnina (s celistvým mocnitelem) *mají od nynějška pro nás obecný smysl*, že to může být cokoli, na co se vztahují zákony (axiomy) grupy (v daném případě tedy také to, co s násobením čísel nemá co dělat). Abychom to ozřejmili hodně drastickým způsobem, připomeňme si, že rovněž např. celá kladná i záporná čísla včetně nuly tvoří vzhledem k *sečítání* grupu, tzv. *aditivní grupu celých čísel*. Zde se „násobením" grupy rozumí obyčejné sečítání, jednotkovým prvkem je obyčejná nula a inversním prvkem k celému číslu a je číslo — a. Aditivní grupa celých čísel je tedy komutativní (Abelova) nekonečná grupa; axiomy grupy (1), (2), (3), (4) a (5) jsou tu známými základními početními zákony pro sečítání. (Podobně je tomu ovšem pro lomená nebo i reálná čísla.)

Možná, že se čtenář zeptá, proč se tedy neužívá pro úkon ve smyslu axiomů grupy názvosloví vzatého ze sčítání místo z násobení nebo vůbec nějakého jiného „neutrálního" názvosloví. Skutečně někteří matematikové užívají tzv. sečítací (aditivní) symboliky a názvů i pro některé nekomutativní grupy, ale všeobecně to není přijímáno. Jak z formálních důvodů jednoduchého psaní, tak i vzhledem k tzv. reprezentacím grup grupami matic (o tom viz v dalším), u nichž jde o skutečné a obecně nekomutativní násobení (na rozdíl od sečítání matic) se jeví historickým vývojem ustálené „násobící" názvosloví a symbolika obecné teorie grup oprávněnou.

Pojem a teorie geometrické pravidelnosti, z nichž jsme vyšli, se jeví z obecného stanoviska, na něž hodláme vystoupit, jako zcela speciální aplikace abstraktní teorie grup, vedle ohromné rozmanitosti jiných aplikací a projevů grupové zákonitosti v přírodních i matematických zjevech. O tom si učiníme obraz na následujících příkladech grup.

Příklad 1. Grupa všech permutací konečně mnoha předmětů (Symetrická grupa)

Mějme n předmětů, jež si pro jednoduchost vždy můžeme nahradit čísly 1, 2, 3, ..., n. Jestliže nahradíme současně každé z napsaných čísel opět některým z těchto čísel, řekněme číslo i ($1 \leqq i \leqq n$) číslem $\pi(i)$ tak, že dvě různá čísla $i \neq j$ jsou nahrazena vždy dvěma různými čísly $\pi(i) \neq \pi(j)$, pak takovému současnému zastoupení π říkáme *permutace.* Je třeba si povšimnout, že někdy se se slovem permutace (n čísel) spojuje jen představa nového *pořadí* $\pi(1), \pi(2), \pi(3), \ldots, \pi(n)$; zde však slovem permutace rozumíme onu *změnu*, která k takovému novému pořadí vede, to jest permutace π je současné nahrazování čísla 1 číslem $\pi(1)$, čísla 2 číslem $\pi(2)$ atd., což samo může být uvažováno bez ohledu na jakékoli pořadí.

Chceme-li vypsat určitou permutaci, uvedeme do první řádky číslice v přirozeném pořadí a pod ně do druhé řádky postupně ty číslice, kterými nahrazujeme při dané permutaci číslice nad nimi. Např.

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

značí totéž co rovnosti

$$\pi(1) = 2,\ \pi(2) = 3,\ \pi(3) = 1$$

$$\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$$

značí totéž co rovnosti

$$\varrho(1) = 2,\ \varrho(2) = 3,\ \varrho(3) = 1,\ \varrho(4) = 4,\ \varrho(5) = 6,\ \varrho(6) = 5$$

(Mohli bychom ovšem stejně dobře psát

$$\pi = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\varrho = \begin{pmatrix} 4 & 5 & 6 & 2 & 3 & 1 \\ 4 & 6 & 5 & 3 & 1 & 2 \end{pmatrix}$$

nahrazování samo, to jest permutaci, tím neměníme.)

Místo permutace n čísel říkává se také permutace stupně n. Dvě permutace téhož stupně lze v určeném pořadí „znásobit". Násobením v určitém pořadí dvou daných permutací rozumíme jejich provedení po sobě v pořadí právě obráceném. Přesněji řečeno, umluvíme si, že jestliže permutace π převádí číslo i v číslo $\pi(i)$ a permutace ϱ (téhož stupně) převádí číslo $\pi(i)$ v číslo $\varrho(\pi(i))$, pak permutace, kterou označme jako $\varrho\pi$, převádí číslo i v číslo $\varrho(\pi(i))$. Součin $\varrho\pi$ je opět permutace stupně n (přitom zdánlivá nesrovnalost v pořadí obou značek π a ϱ má svoje výhody a je dána matematicky nepodstatnou okolností, že jsme běžně zvyklí číst odleva doprava, ale psát permutované — nahrazované — číslo i napravo od permutace π).[4]) Např. je-li

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

a

$$\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

pak

$$\varrho\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

[4]) Kdybychom se této nesrovnalosti chtěli vyhnout, museli bychom psát permutované číslo před permutaci, tedy $(i)\pi$, místo $\pi(i)$, což by bylo méně vhodné.

Nyní si dokažme, že *permutace stupně n tvoří vzhledem k uvedenému násobení grupu, tzv. symetrickou grupu* S_n, *která je řádu* $n! = 1.2.3 \ldots n$.

(1) Axiom (zákon) neomezené jednoznačnosti násobení je podle definice samozřejmě splněn.

(2) Axiom asociativity žádá, aby při libovolných třech permutacích π, ϱ, σ číslo $\sigma(\varrho\pi(i))$ bylo totéž jako číslo $\sigma\varrho(\pi(i))$, a to při jakémkoli i. Skutečně, dle naší definice násobení permutací jsou obě čísla rovna číslu $\sigma(\varrho(\pi(i)))$.

(3) Axiom jednotkového prvku je zřejmě splněn: jednotkovým prvkem je tzv. identická permutace ι (čti jota) tvaru

$$\iota = \begin{pmatrix} 1 & 2 & 3 \ldots n \\ 1 & 2 & 3 \ldots n \end{pmatrix}, \quad \iota(i) = i$$

(4) Axiom inversního prvku je splněn, neboť zřejmě inversní permutací k permutaci π je prostě permutace, označme ji π^{-1}, převádějící číslo $j = \pi(i)$ v číslo $i = \pi^{-1}(j)$. Vzpomeneme-li si ještě ze střední školy, že všech pořadí z n čísel je $n! = 1.2.3 \ldots n$ (n — faktoriál), a že tedy bude i tolik permutací, kterými se tato pořadí ze základního dají vytvořit, přesvědčili jsme se o platnosti celého našeho tvrzení.

Grupy permutací jsou důležité teoreticky i v aplikacích, v matematice i v přírodě. Lze říci, že v moderní matematice na poč. XIX. století se pojem grupy objevil v grupách permutací, a to přímo v aplikaci na teorii algebraických rovnic libovolného celistvého kladného stupně o jedné neznámé. (O této tzv. *Galoisově*[5]) teorii

[5]) J. E. Galois, který předčasně zahynul v souboji, byl geniálním francouzským matematikem z počátku XIX. stol. (Zemřel ve věku 21 let.)

rovnic najde čtenář zmínku ve Schwarzově knížce „O rovnicích", sbírce ve „Cesta k vědění"; pro základní pojmy Galoisovy teorie viz např. Kurošovu učebnici.)[6])

Příklad 2. Grupa geometrických transformací

Pro geometrii (i fyziku) je zásadně důležitý pojem *grupy geometrických* (popř. fyzikálních) *pohybů* čili transformací.[7]) Tento pojem si objasníme na příkladě ze školy známých *euklidovských pohybů roviny*.

Představme si, že se tuhá rovina, unášející kartézskou soustavu souřadnic *Oxy*, pohnula v sobě samé, tj. aniž se kterýkoli bod této roviny dostal mimo ni. Pak změnu polohy (pohyb) této roviny budeme posuzovat vzhledem k výchozímu postavení soustavy souřadnic. Bod, který měl *původně* úsečku[8]) hodnoty řekněme x' a pořadnici[8]) hodnoty řekněme y' (jež se po pohybu objevují a odečítají v *nové* poloze soustavy souřadnic), dospěl do místa bodu, jehož úsečka obnáší x a jehož pořadnice obnáší y (obojí měřeno v původní poloze soustavy souřadnic). „Nové" souřadnice bodu x, y lze vyjádřit „starými" souřadnicemi x', y' ze školy známými tzv. transformačními vzorci

---

[6]) Jde o monografii významného sovětského matematika *A. G. Kuroše*, který dlouhá léta vedl moskevský algebraický seminář založený *O. J. Šmidtem* (známým veřejnosti asi více jako polární badatel). Nedávno zemřelý prof. Kuroš byl velkým přítelem Československa.

[7]) Srov. s vysvětlením geometrického rázu pojmu pohybu drobným tiskem v 1.kap.

[8]) Termín „úsečka" se zde užívá ve smyslu „1. souřadnice" nebo „x-ová souřadnice" a podobně termín „pořadnice" ve smyslu „2. souřadnice" čili „y-ová souřadnice". Jde o starší termíny, které však pro zachování původního rázu textu byly na tomto místě ponechány.

$$x = x' \cos \alpha - y' \sin \alpha + a$$
$$y = x' \sin \alpha + y' \cos \alpha + b$$

kde α je proti ručkám hodin kladně měřený úhel otočení (určený až na celistvý násobek plného úhlu 2π v míře obloukové), tj. úhel od staré polohy osy úseček k její nové poloze, a a b jsou souřadnice bodu, do něhož se dostal po pohybu počátek 0 soustavy souřadnic.

Tyto *závislosti* nových souřadnic na starých (které ve svém úhrnu označme $T(\alpha, a, b)$), popisují a definují tzv. euklidovskou transformaci, čili **euklidovský pohyb roviny**. Každý euklidovský pohyb T je plně určen uspořádanou trojicí čísel α, a, b — tzv. svými **parametry**. Způsob, jakým si označíme (staré či nové) souřadnice je lhostejný, je třeba jen vědět, které souřadnice jsou staré a které nové, která z nich je úsečkou a která pořadnicí; jinak se volba označení souřadnic řídí jen zřetely formální (početní) účelnosti.

Zvláštními případy euklidovského pohybu roviny jsou: čistý posuv (pro $\alpha = 0$) a čisté otočení (pro $a = b = 0$); obecný případ je kombinací obou (při čemž pozor na pořadí, viz níže).

Předepišme si obecně jiný euklidovský pohyb roviny, o parametrech α', a', b', který účelně vypišme takto:

$$x' = x'' \cos \alpha' - y'' \sin \alpha' + a'$$
$$y' = x'' \sin \alpha' + y'' \cos \alpha' + b'$$

Představme si, že jsme oba pohyby složili v jeden tím, že jsme provedli nejprve pohyb $T'(\alpha', a', b')$ a pak pohyb $T(\alpha, a, b)$. Výsledkem musí ovšem být opět euklidovský pohyb $T''(\alpha'', a'', b'')$, což dokážeme a jeho parametry α'', a'', b'' nalezneme prostě tak, že dosadíme do rovnic, určujících T z rovnic určujících T'. (Kdybychom si nebyli vhodně označili souřadnice, museli bychom si je

vhodně přejmenovat před početním složením obou pohybů.) Máme

$$x = (x'' \cos \alpha' - y'' \sin \alpha' + a') \cos \alpha - (x'' \sin \alpha' + y'' \cos \alpha' + b') \sin \alpha + a = x''(\cos \alpha' \cos \alpha - \sin \alpha' . \sin \alpha) - y''(\sin \alpha' \cos \alpha + \cos \alpha' \sin \alpha) + a' \cos \alpha - b' \sin \alpha + a = x'' \cos(\alpha' + \alpha) - y'' \sin(\alpha' + \alpha) + a' \cos \alpha - b' \sin \alpha + a$$

Podobně

$$y = x'' \sin(\alpha' + \alpha) + y'' \cos(\alpha' + \alpha) + a' \sin \alpha + b' \cos \alpha + b$$

takže $\alpha'' = \alpha + \alpha'$ (úhel otočení výsledného pohybu je součtem obou úhlů otočení) a

$$a'' = a' \cos \alpha - b' \sin \alpha + a$$
$$b'' = a' \sin \alpha + b' \cos \alpha + b$$

(Počátek se prvým pohybem T' dostal do bodu a', b' a tento bod dostal se dalším pohybem T do bodu a'', b''.)[9])

Skládání euklidovských pohybů roviny lze tedy stručně vystihnout rovností

$$T(\alpha, a, b)\, T'(\alpha', a', b') = T''(\alpha + \alpha', a' \cos \alpha - b' \sin \alpha + a, a' \sin \alpha + b' \cos \alpha + b)$$

(Podobně jako při násobení permutací zaznamenáváme v součinu dvou geometrických transformací postup

[9]) Na střední škole se při geometrickém odvozování součtové poučky pro sin a cos (jíž jsme tu užili při odvození parametrů výsledného pohybu) vyhází naopak z geometricky názorného faktu, že úhel dvou po sobě následujících euklidovských otočení je roven součtu obou úhlů, a z geometrického znázornění otočení se vyvodí součtové poučky pro sin a cos.

skládaných pohybů zprava doleva; hlubším důvodem pro toto nezvyklé psaní je okolnost, že zobecnění pojmu permutace na nekonečné soubory předmětů, jako jsou např. body roviny, zahrnuje v sobě i pojem geometrické (euklidovské) transformace roviny jako zvláštní případ. Permutovanými předměty jsou pak na místě celých čísel uspořádané dvojice reálných čísel (kde prvé číslo je úsečkou, druhé pořadnicí bodu) a euklidovský pohyb jakožto předepsané nahrazení starých souřadnic bodu, tj. dvojice $[x', y']$ novými souřadnicemi téhož bodu, tj. dvojicí $[x, y]$, se opravdu jeví jako jistá „permutace" bodů roviny, rozumí se ovšem nikoli ve středoškolském, nýbrž ve shora uvedeném smyslu slova.)

Snadno se dá ukázat,[10]) že euklidovské pohyby možno považovat za prvky grupy, že totiž platí i pro skládání euklidovských pohybů, považované za „násobení", v tzv. *grupě euklidovských pohybů* roviny, axiomy (1) až (4). Tato grupa je nekomutativní a nekonečná. (Neplatnost komutativního zákona již při obrácení sledu čistého posuvu a čistého otočení zná každý, kdo ví, že vpravo v bok a pak krok vpřed dá něco jiného, než krok vpřed a pak vpravo v bok.)

Ke grupě euklidovských pohybů roviny (včetně překlápění) můžeme dospět i jiným, méně názorným způsobem: Je to totiž právě ta grupa (tzv. lineárních transformací či permutací) bodů[11]) roviny, která zachovává

---

[10]) Přenechávám to čtenářově píli; asociativní zákon se nejlépe bez počítání dokazuje na základě předchozí poznámky, že pohyb roviny je permutace jejích bodů. (Asociativní zákon pro konečné permutace známe.)

[11]) Lineární se nazývá transformační závislost, v níž se souřadnice vyskytují nanejvýš v první mocnině. (Název podle lat. linea recta = přímka, v jejíž rovnici se vyskytují souřadnice rovněž nejvýš v první mocnině.)

vzdálenost dvou bodů, což ústí v požadavek, aby dva body x_1, y_1 a x_2, y_2 vždy přešly ve dva body x_1', y_1' a x_2', y_2'

$$V = +\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} =$$
$$+$$
$$= +\sqrt{(x_1' - x_2')^2 + (y_1' - y_2')^2}$$
$$+$$

Říkáme, že funkce V souřadnic je invariantem vůči (lineární) grupě transformací euklidovských. (Grupa se nazývá lineární, jestliže transformační závislosti jsou lineární.)

Jestliže určíme za definující invariant jinou vhodnou funkci souřadnic, dostáváme lineární grupu jiných, tzv. neeuklidovských „pohybů" roviny, odpovídajících „neeuklidovské" geometrii. Důležitost teorie invariantů vůči grupám transformací pro obecné geometrické úvahy je tak veliká, že německý matematik *F. Klein* přímo definoval geometrii jako studium invariantů vůči grupám transformací.

Ve fyzice poznáme význam obecné teorie grup transformací s daným invariantem na tomto příkladě: Z požadavku speciální teorie relativity, že světelný signál se má šířit stejnou a nepřekročitelnou rychlostí na všechny strany nejen vzhledem ke zdroji světla (což je samozřejmé) nýbrž i v soustavě, která se vzhledem ke zdroji pohybuje přímočaře rovnoměrně, vyplývá (v nejjednodušším případě posuvu osy x v sobě) požadavek invariance (neměnosti) funkce $x^2 - c^2t^2$ (při lineární transformaci starých „souřadnic" novými); „souřadnice" t má tu význam času, c značí rychlost světla.

Tímto invariantem je definována jistá lineární grupa (neeuklidovských) transformací, tzv. grupa *Lorentzova*. Její studium je matematickým základem speciální teorie relativity. (Viz cvič. 10 ke kap. 4.)

Příklad 3. Grupa lineárních homogenních transformací (grupa matic)

Zaveďme si ve vzorci pro čisté euklidovské otočení (viz předchozí příklad) toto označení (z důvodů, jež budou ihned zřejmé):

$$a_{11} = \cos \alpha,\ a_{12} = -\sin \alpha,\ a_{21} = \sin \alpha,\ a_{22} = \cos \alpha$$

Pak vyjádření euklidovského otočení má tvar

$$\begin{aligned} x &= a_{11}x' + a_{12}y' \\ y &= a_{21}x' + a_{22}y' \end{aligned}$$

Podobně kdybychom sledovali euklidovská otočení prostoru, nalezli bychom pro závislost nových prostorových souřadnic x, y, z na starých prostorových souřadnicích x', y', z' téhož bodu vzorce

$$\begin{aligned} x &= a_{11}x' + a_{12}y' + a_{13}z' \\ y &= a_{21}x' + a_{22}y' + a_{23}z' \\ z &= a_{31}x' + a_{32}y' + a_{33}z' \end{aligned}$$

kde pevné číslo (tzv. koeficient) a_{ik} stojící v i-tém řádku a k-tém sloupci pravé strany napsaného vzorce je kosinus úhlu, který svírá i-tá souřadnicová osa v původní poloze s k-tou souřadnicovou osou v nové poloze. (i, k znamená některé z čísel 1, 2, 3; např. a_{13} je kosinus úhlu mezi starou polohou osy x-ové a novou polohou osy z-ové.)

Euklidovská otočení roviny, resp. prostoru jsou příklady tzv. lineárních homogenních[12]) transformací. Tímto pojmem, který má velikou důležitost v celé matematice, geometrii a i v teoretické fyzice, rozumíme obecně souhrn závislostí n závisle proměnných čísel $x_1, x_2, x_3, \ldots, x_n$ na m daných (nezávislých) proměnných číslech $x_1', x_2', x_3', \ldots, x_m'$ takových, že je lze napsat ve tvaru

$$A = \begin{cases} x_1 = a_{11}x_1' + a_{12}x_2' + \ldots + a_{1m}x_m' \\ x_2 = a_{21}x_1' + a_{22}x_2' + \ldots + a_{2m}x_m' \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = a_{n1}x_1' + a_{n2}x_2' + \ldots + a_{nm}x_m' \end{cases}$$

Koeficienty transformace, pevná čísla a_{ik}, svou hodnotou (při daných hodnotách tzv. řádkového indexu i a tzv. sloupcového indexu k) plně určují svým souhrnem takovou lineární homogenní transformaci, kdežto označení proměnných (nikoli jejich pořadí) je lhostejné. V dalším se omezíme na lineární homogenní transformace, kde je týž počet závislých i nezávislých proměnných, tedy kde $m = n$ a dále takových, že z předpokládaných hodnot závisle proměnných $x_1, x_2, \ldots, x_n$ lze k nim vypočíst (jednoznačně) hodnoty závisle proměnných, tj. řešit transformační rovnice podle neznámých $x_1', x_2', \ldots, x_n'$. (Některý čtenář ví, že nutná a postačující podmínka takové řešitelnosti transformačních rovnic A je ta, aby tzv. determinant soustavy byl číslem od nuly různým.[13])

[12]) Homogenní (česky = stejnorodý) zde značí, že všechny sčítance obsahují nezávisle proměnné (není tzv. absolutního členu).

[13]) O determinantech se čtenář poučí v každé základní učebnici (klasické) algebry, anebo přímo v učebnici B. Bydžovského: Úvod do teorie determinantů a matic, JČMF Praha.

Neznámé $x_1', x_2', \ldots, x_n'$ lze tedy vyjádřit lineární homogenní závislostí na daných hodnotách $x_1, x_2, \ldots, x_n$, čili lze nalézt tzv. inversní (lineární homogenní) transformaci. Máme tedy na mysli jen lineární homogenní transformace, které mají k sobě (lineární homogenní) transformaci inversní.

Podobně jako při geometrických transformacích (příklad 2) budeme definovat i skládání lin. hom. transformací (téhož počtu proměnných) jejich postupným prováděním. Předvedeme si to na příkladě $n = 3$. Mějme dvě takové lineární homogenní transformace.[14])

$$A = \begin{cases} x_1 = a_{11}x_1' + a_{12}x_2' + a_{13}x_3' \\ x_2 = a_{21}x_1' + a_{22}x_2' + a_{23}x_3' \\ x_3 = a_{31}x_1' + a_{32}x_2' + a_{33}x_3' \end{cases}$$

$$B = \begin{cases} x_1' = b_{11}x_1'' + b_{12}x_2'' + b_{13}x_3'' \\ x_2' = b_{21}x_1'' + b_{22}x_2'' + b_{23}x_3'' \\ x_3' = b_{31}x_1'' + b_{32}x_2'' + b_{33}x_3'' \end{cases}$$

Složenou transformací AB (čili součinem AB obou transformací) rozumíme vyjádření závisle proměnných x_1, x_2, x_3 transformace A nezávisle proměnnými x_1'', x_2'', x_3'' transformace B, což se provede dosazením za x_1', x_2', x_3' z rovnic pro B do rovnic pro A. Po příslušné úpravě vytýkáním dostáváme (provedení přenecháváme čtenáři jako snadné cvičení):

[14]) Číselné příklady najde čtenář níže — zde by však provádění skládání transformací spíše zatemnily, než objasnily.

$$AB = \begin{cases} x_1 = (a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31})x_1'' + (a_{11}b_{12} + \\ \quad + a_{12}b_{22} + a_{13}b_{32})x_2'' + (a_{11}b_{13} + a_{12}b_{23} + \\ \quad + a_{13}b_{33}).x_3'' \\ x_2 = (a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31})x_1'' + (a_{21}b_{12} + \\ \quad + a_{22}b_{22} + a_{32}b_{23})x_2'' + (a_{21}b_{13} + a_{22}b_{23} + \\ \quad + a_{23}b_{33}).x_3'' \\ x_3 = (a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31})x_1'' + (a_{31}b_{12} + \\ \quad + a_{32}b_{22} + a_{33}b_{32})x_2'' + (a_{31}b_{13} + a_{32}b_{23} + \\ \quad + a_{33}b_{33}).x_3'' \end{cases}$$

Součin AB obou lineárních homogenních transformací je tedy opět lineární homogenní transformace; jeho tvoření si zapamatujeme, když si uvědomíme, že v i-tém řádku a k-tém sloupci pravé strany transformace AB se nalézá „součin i-tého řádku z A s k-tým sloupcem z B" (čtenář jistě pochopí bez dlouhého popisování, co se míní zkráceným rčením v uvozovkách).

Při právě definovaném násobení všechny ty lineární homogenní transformace třech — a obecně n proměnných, které mají k sobě inversní (lineární homogenní) transformaci, tvoří grupu, tzv. homogenní *lineární grupu n-tého stupně*; při tom však je třeba ještě udat druh koeficientů, které vystupují v transformacích grupy, tj. zda jsou to čísla racionální, reálná či dokonce komplexní. (Podrobné ověření platnosti axiomů grupy musíme zde vynechat; čtenář je najde v každé učebnici vyšší algebry.)

Protože, jak jsme již zdůraznili, lim. hom. transformace je úplně dána svými koeficienty, můžeme místo násobení transformací hovořit prostě o „násobení" celých souhrnů příslušných koeficientů (jako celků). Těmito souhrny koeficientů rozumíme jejich hodnoty v charakteristickém čtvercovém uspořádání tvaru

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

a říkáme jim *regulární matice* n-tého stupně (n-řadové) koeficientů příslušné lineární homogenní transformace, přičemž dodatek „koeficientů…" zpravidla vynechávame a mluvíme prostě o regulárních maticích stupně n; slovo regulární (pravidelný) vyznačuje právě onu předpokládanou vlastnost příslušné lineární homogenní transformace, že k ní existuje transformace inversní (dle poznámky nahoře lze též říci, že matice je regulární, je-li determinant z jejích koeficientů různý od nuly).

Matici (stupně n), mající v i-tém řádku a k-tém sloupci číslo a_{ik}, pak označujeme stručně jako (a_{ik}) (je-li záhodno, s dodatkem $i, k = 1, 2, 3, \dots, n$).
Součinem matice $A = (a_{ik})$ násobené zprava maticí $B = (b_{ik})$ rozumíme tedy matici $AB = C = (c_{rs})$, kde

$$c_{rs} = a_{r1}b_{1s} + a_{r2}b_{s2} + \dots + a_{rn}b_{ns}; \; r, s = 1, 2, \dots, n$$

Tím je definována *grupa (regulárních) matic stupně n (n-řadových)*.

Mezi maticemi (jakožto čtvercovými schématy čísel) a příslušnými lineárními homogenními transformacemi je zhruba řečeno (srovnej další odst.) jen ten rozdíl, že uvažovat matice místo příslušné transformace je přirozeným zjednodušením, jestliže nám jde spíše o násobení (skládání) transformací než o jejich samotné provádění.

Jednotkovým prvkem je tu tzv. jednotková matice

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

mající vesměs jednotky v hlavní úhlopříčce a nuly na ostatních místech. Jednotková matice přísluší k identické transformaci

$$x_1 = x_1', x_2 = x_2', \ldots, x_n = x_n'$$

(Z definice násobení matic snadno vidět, že násobení jednotkovou maticí danou matici nezmění.) Několik číselných příkladů čtenáři pomůže překonat případné počáteční potíže či nedorozumění.

a) Jestliže stupeň matice je $n = 1$, pak regulární matice jsou prostě čísla různá od nuly. (Matice se skládá z jediného koeficientu, řekněme $a_{11} = a$, nebo $b_{11} = b$ apod.) Násobení matic je prostě násobením čísel. Příslušné homogenní transformace jsou ty nejjednodušší lineární závislosti, řekněme

$$A = \{x = ax'\}, B = \{x' = bx''\},$$
$$AB = \{x = abx''\}$$

apod.

Grupa matic stupně 1 je tedy prostě multiplikativní grupa jejich koeficientů.

b) Položme $n = 2$. Nechť např.

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} \frac{1}{2} & 0 \\ 1 & 2 \end{pmatrix}$$

Pak

$$AB = \begin{pmatrix} 1.\frac{1}{2} + 2.1 & 1.0 + 2.2 \\ 3.\frac{1}{2} + 4.1 & 3.0 + 4.2 \end{pmatrix} = \begin{pmatrix} \frac{5}{2} & 4 \\ \frac{11}{2} & 8 \end{pmatrix}$$

Matice AB přísluší k součinu (složení lineární homogenní transformace)

$$x_1 = x_1' + 2x_2'$$
$$x_2 = 3x_1' + 4x_2'$$

s transformací (pro niž schválně volme jiný způsob označení proměnných, abychom si uvědomili jeho nepodstatnost)

$$x = \tfrac{1}{2}x'$$
$$y = x' + 2y'$$

c) Hledejme inversní matici k matici

$$A = \begin{pmatrix} 1 & 2 & 0 \\ -2 & -4 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Máme tedy nalézt matici X tak, aby

$$\begin{pmatrix} 1 & 2 & 0 \\ -2 & -4 & 0 \\ 1 & 1 & 1 \end{pmatrix} . X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

To dle předchozího znamená rozřešit příslušné transformační rovnice

$$\begin{aligned} x_1 &= x_1' + 2x_2' \\ x_2 &= -2x_1' - 4x_2' \\ x_3 &= x_1' + x_2' + x_3' \end{aligned}$$

pro neznámé x_1', x_2', x_3' za předpokladu, že čísla x_1, x_2, x_3 jsou libovolně dána, a vyjádřit tak lineární homogenní závislost (inverzní transformaci) proměnných čárkovaných na proměnných nečárkovaných.

Abychom se případně zbytečně nenamáhali, je dobře vyzkoumat, zda napsané rovnice mají vůbec řešení (pro každé x_1, x_2, x_3). Vidíme však, že přičteme-li k dvojnásobku první rovnice druhou rovnici, dostáváme rovnost $2x_1 + x_2 = 0$. To je v rozporu s libovolnou volitelností a tedy se vzájemnou nezávislostí proměnných x_1 a x_2. Lze tedy napsané rovnice řešit dle čárkovaných neznámých jen tehdy, jestliže je splněna podmínka $2x_1 + x_2 = 0$ (což obecně není), takže inversní transfor-

mace k transformaci o dané matici A neexistuje; matice A není regulární a není tedy prvkem naší grupy (lineární grupy matic stupně 3 s racionálními koeficienty). (Čtenář, znalý základů teorie determinantů to ví předem, neboť si všimne, že determinant dané matice A je nula, protože druhý řádek matice je 2-kráte vzatý první řádek.)

d) Vezměme si místo matice A matici

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 3 \\ 1 & 2 & 0 \end{pmatrix}$$

a hledejme k ní inversní matici, tj. hleďme vypočíst hodnoty čárkovaných proměnných pomocí nečárkovaných z rovnic

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

Řešení je, jak se čtenář snadno přesvědčí

$$\begin{aligned} x' &= x \\ y' &= -\tfrac{1}{2}x \qquad + \tfrac{1}{2}z \\ z' &= -\tfrac{1}{3}x + \tfrac{1}{3}y \end{aligned}$$

Tedy inversní matice

$$B^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 3 \\ 1 & 2 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{3} & \frac{1}{3} & 0 \end{pmatrix}$$

Skutečně, znásobení obou matic dává

$$BB^{-1} = \begin{pmatrix} 1.1 + 0.(-\frac{1}{2}) + 0.(-\frac{1}{3}) & 1.0 + 0.0 + 0.\frac{1}{3} \\ 1.1 + 0.(-\frac{1}{2}) + 3.(-\frac{1}{3}) & 1.0 + 0.0 + 3.\frac{1}{3} \\ 1.1 + 2.(-\frac{1}{2}) + 0.(-\frac{1}{3}) & 1.0 + 2.0 + 0.\frac{1}{3} \end{pmatrix}$$

$$\begin{pmatrix} 1.0 + 0.\frac{1}{2} + 0.0 \\ 1.0 + 0.\frac{1}{2} + 3.0 \\ 1.0 + 2.\frac{1}{2} + 0.0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Přehlédnuvše v předchozích třech příkladech nejdůležitější druhy grupového násobení, obraťme se ještě ke dvěma příkladům grup zcela jiného druhu.

Příklad 4. Grupa idealizovaných barev

Za prvky této grupy pokládáme barvy v jejich duhové čistotě, za grupové násobení mísení barev (bez ohledu na jejich pořadí, půjde tedy o grupu komutativní).

Předpokládejme tři základní barvy v základní síle, tj. modř M, červeň $Č$ a žluť $Ž$ tak, že smíšením těchto tří barev vznikne čirá (neutrální) barva N. K přibližné realizaci poslouží známý barevný kotouč, rozdělený na tři stejně veliké výseče, modrou, červenou, žlutou, na němž se dojem neutrální, ve skutečnosti šedivě špinavé směsi N docílí rychlým otáčením. Mísením základních tří barev lze (teoreticky) docílit všech barevných odstínů jen tehdy, když jsou základní intenzity modré, červené a žluté dosti jemné. Mísení barev, ovšem v příslušné idealizaci, podléhá zákonům komutativní grupy, v níž neutrální barva N je jednotkovým prvkem a doplňková barva je prvkem inversním. Tak např. můžeme psát $M.Č.Ž = N$ čili $Ž^{-1} = M.Č$ (tj. doplňková barva ke žluti je „součin" $M.Č$, což je fialová barva v základní síle). $Č^2.Ž$ je oranžová červenavého odstínu, $M^5.Č$ je modř se slabě fialovým nádechem (při čemž čtenář vidí, že symbolika teorie grup je s to vyjádřit barevné odstíny mnohem přesněji, než obvyklá názvoslovní nauky o barvách).

Příklad 5. Booleova grupa

Mějme jakýkoli počet předmětů, např. 4 předměty, nazvané a, b, c, d. Utvořme všechny podmnožiny množiny $\{a, b, c, d\}$; těch je $2^4 = 16$ (včetně prázdné množiny $\emptyset$ a množiny $\{a, b, c, d\}$). Těchto 16 množin budeme pova-

žovat za prvky grupy s „násobením" definovaným takto: za součin $X.Y$ dvou množin X a Y budeme považovat množinu skládající se ze všech předmětů (prvků), které se vyskytují právě v jedné z uvažovaných množin.[15]) Tak např. jestliže $X = \{b, c, d\}$ a $Y = \{a, b, c\}$, je $X.Y = \{a, d\}$. Kdyby bylo Y rovno $\{c, d\}$, platilo by $X.Y = \{b\}$.

Axiomy teorie grup jsou tu splněny (jak se čtenář sám může přesvědčit; větší námahu mu dá jen ověření platnosti axiomu asociativnosti). Jednotkovým prvkem je $\emptyset$, inversní množinou k množině X je tato množina sama, je $X^{-1} = X$, neboť platí (podle definice násobení v naší grupě) $X.X = X^2 = \emptyset$ pro každé X (což není nic zvláštního, i při násobení čísel máme $-1^{-1} = -1$).

Této grupě, která je Abelova a při n daných předmětech má 2^n prvků, to jest skupin z daných předmětů, a která při nekonečně mnoha daných předmětech je ovšem nekonečná, se říká *Booleova* [16]) *grupa*.

Cvičení

1. Upravte na „normální tvar"

$$\begin{pmatrix} 1 & 2 & 3 & \dots \\ \cdot & \cdot & \cdot & \dots \end{pmatrix}, \text{ resp. } \begin{pmatrix} a & b & c & \dots \\ \cdot & \cdot & \cdot & \dots \end{pmatrix}$$

$(X-Y) \cup (Y-X) = (X \cup Y) - (Y \cap X)$

[15]) Čtenář znalý množinové symboliky ihned vidí, že lze psát $X.Y = (X \cup Y) - (X \cap Y)$.

[16]) G Boole byl anglický matematik z poloviny XIX. stol., který vedle základních prací o tzv. diferenčním počtu proslul zavedením algebraického způsobu uvažování do teoretické logiky, čímž se stal jedním ze zakladatelů moderní matematické logiky.

permutace

$$\begin{pmatrix}5&2&1&4&3\\1&4&3&5&2\end{pmatrix},\ \begin{pmatrix}2&6&5&7&3&1&4\\3&5&2&6&1&4&7\end{pmatrix},\ \begin{pmatrix}d&b&e&f&a&c\\e&a&f&b&c&d\end{pmatrix},\ \begin{pmatrix}c&d&a&b\\a&d&c&b\end{pmatrix}$$

2. $\begin{pmatrix}1&2&3&4&5&6\\4&5&2&1&3&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&1&6&4&2&3\end{pmatrix} = ?, \begin{pmatrix}1&2&3&4&5\\5&2&4&1&3\end{pmatrix}^4 = ?,$

$\begin{pmatrix}1&2&3&4&5\\5&2&4&1&3\end{pmatrix}^{101} = ?, \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}^{-1} = ?$

3. Řešte rovnice (pro neznámé permutace X)

$$X\begin{pmatrix}a&b&c&d&e\\c&a&b&e&d\end{pmatrix} = \begin{pmatrix}a&b&c&d&e\\e&a&c&b&d\end{pmatrix},\ \begin{pmatrix}a&b&c&d&e\\c&a&b&e&d\end{pmatrix}X = \begin{pmatrix}a&b&c&d&e\\e&a&c&b&d\end{pmatrix}$$

4. Určete euklidovský pohyb roviny pomocí parametrů, vzniklý otočením o 30°, následovaným posuvem $x' = x + 2$, $y' = y - 3$ a ještě následovaný otočením o —60°.

5. Řešte v grupě euklidovských pohybů roviny rovnici

$$T(30°.\ 1,\ 2)\ X = T(-90°;\ -2,5)$$

o neznámé — pohybu X.

6. Vypočtěte

$$\begin{pmatrix}1&0&3\\2&1&-2\\5&0&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&2&3\\1&2&3\end{pmatrix} = ?, \begin{pmatrix}1&2&-3&4\\0&3&-4&1\\0&0&1&0\\0&0&0&2\end{pmatrix}^2 = ?, \begin{pmatrix}1&2&-3&4\\0&3&-4&1\\0&0&1&0\\0&0&0&2\end{pmatrix}^{-1} = ?$$

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\\1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} = ?$$

7. Ukažte, že při násobení libovolných ne nutně regulárních dvou matic stupně alespoň 2 se může stát, že dva činitelé různí od nulové matice (ze samých nul) mohou dát nulovou matici jako součin.

8. *Nechť M je libovolná množina o n prvcích; uvažujme všechny podmnožiny množiny M a definujme pro ně násobení tak, že součinem dvou libovolných podmnožin je množina skládající se ze všech těch prvků, jež buď leží v obou daných

podmnožinách anebo neleží v žádné z nich. Ukažte, že systém všech podmnožin množiny M vzhledem k tomuto násobení tvoří grupu. (Jednotkovým prvkem je množina M.)

9. *Dokažte, že grupa, v níž platí $x^2 = j$ (j jednotka grupy) pro každý prvek x, je komutativní. (Uvažte že $x^{-1} = r$ platí pro každý prvek z.)

10. *Dokažte, že homogenní lineární transformace dvojice proměnných x, t ve dvojici proměnných x', t' dané rovnicemi tvaru

$$T(v) = \begin{cases} x' = k(x - vt) \\ t' = k\left(t - \frac{v}{c^2}x\right), \end{cases} \qquad \left(k = \frac{1}{\sqrt{1 - \frac{v^2}{c^2}}}\right)$$

kde c je konstanta, v je parametr, $|v| \leqq |c|$ tvoří grupu, tzv. Lorentzovu grupu speciální teorie relativity. [$c \doteq 3.10^{10}$ cm/sec je stálá rychlost světla ve vakuu, x, t jsou délka a čas (v cm a sec) na relativně klidné přímce a; x', t' jsou délka a čas na relativně pohybované přímce a' rychlostí v (stálou) a rovnoběžnou s přímkou a.]