

O grupách a svazech

1.3 Obecný pojem grupy. Jiné příklady grup

In: Ladislav Rieger (author): O grupách a svazech. (Czech). Praha: Přírodovědecké vydavatelství, 1952. pp. 15–33.

Persistent URL: <http://dml.cz/dmlcz/403364>

Terms of use:

© Přírodovědecké vydavatelství

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

Přímou praktickou důležitost má theorie grup zákrytových pohybů v krystalografii, t. j. v nauce o geometrické pravidelnosti krystalů,⁷ ať již jde o t. zv. makrokristaly (viditelných rozměrů) nebo o mikrokristaly (neviditelné pouhým okem).

Podobně má theorie grup aplikaci i v chemii, v theorii stereoisomerů, t. j. v nauce o chemických sloučeninách týchž atomů v též počtu, ale lišících se geometrickým uspořádáním v molekule.⁸

Cvičení k 1, 2.

1. $ABCD = ?$, $ABDE = ?$, $A^2B^2 = ?$ Řešte rovnice $AX = E$; $XE = B$, $XB = X^2C$.

2. Najděte další příklady dvojice zákrytových pohybů rovnostranného trojúhelníka, které ukazují neplatnost komutativního zákona.

3. $A^{15} = ?$, $D^{-135} = ?$, $(AD)^{15} = ?$ (Návod: na př. $D^3 = J = D^0$ a pod.; užitě dělení mocnitele se zbytkem!)

4. Přesvědčte se, že v grupě zákrytových pohybů rovnostranného trojúhelníka neplatí vždy poučka: Součin se umocní, umocní-li se jednotliví činitelé. (Najděte pohyby X, Y , aby pro vhodný mocnitel, celistvé n bylo $(XY)^n \neq X^n Y^n$.)

5.*Skládejme po sobě prováděné zákrytové pohyby rovnostranného trojúhelníka tak, že při tom každou osu překlápění považujeme za nehybnou (pevně danou v původní rovině), stejně jako osu ořázení roviny. Takové skládání splňuje 1., 3. a 4. axiom theorie grup, nikoli však 2. axiom asociativity. Přesvědčte se o tom.

6. Sestrojte tabulku pro grupu zákrytových pohybů čtverce. Ukažte, že je to komutativní grupa.

1.3. OBECNÝ POJEM GRUPY. JINÉ PŘÍKLADY GRUP.

K výtčení 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 (na př. kladných zlomků). Avšak ukážeme si, v jak rozmanitých

⁷ Blíží v učebnici Speiserově nebo ve speciální monografii od F. Burekhardta (viz lit. na konci).

⁸ Viz na př. Póly a, Acta Mathematica (1937).

dalších podobách nalézáme splněny tytéž axiomy grupy (1) až (4) z 1,2. K tomu si výslovně uvědomme následující. Axiomy grupy budou splněny vždy nějakým, násobením připomínajícím úkonem, na př. „skládáním“ (pohybů) prováděným s předměty, kterým budeme od nynějška říkat *prvky grupy*. Tyto prvky musí ovšem tvořit vymezený soubor (t. j. *grupu*) tak, že výsledek „násobení“ („složení“) dvou prvků grupy v daném pořadí je opět prvkem grupy. Chceme-li si tedy výslovně formulovat axiomy grupy obecně, vrátíme se do předchozího odstavce 1,2 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, grupové násobení (v grupě) 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 hůdně drastickým způsobem, připomeňme si, že rovněž *sečítání* čísel, na př. celých, kladných i záporných včetně nuly *tvoří grupu*, t. zv. *sečítací* (čili aditivní) *grupu celých čísel*. Zde se „násobením“ grupy rozumí obyčejné sečítání, jednotkovým prvkem je obyčejná nula a inverzním prvkem k celému číslu a je číslo $-a$. Sečítací 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 *sečítání*, místo z *násobení* nebo vůbec nějakého jiného „neutrálního“ názvosloví. Skutečně někteří američtí matematikové užívají t. zv. *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 t. zv. *representacím grup grupami matic* (o tom viz

v dalším), u nichž jde o skutečné a obecně nekomutativní násobení (na rozdíl od sečítání matie) se jeví historickým vývojem ustálené „násobící“ názvosloví a symbolika obecné teorie grup oprávněnou.

Pojem a teorie geometrické pravidelnosti, z nichž jsme vyšli, se jeví s 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 $1, 2, 3, \dots, n$. Jestliže zastoupíme současně každé z napsaných čísel opět některým z těchto čísel, řekněme číslo i ($1 \leq i \leq n$) 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 na střední škole spojujeme se slovem permutace (n čísel) jen představu nového pořadí $\pi(1), \pi(2), \pi(3), \dots, \pi(n)$; 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 vypsát 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. Na př.

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

značí totéž co rovnosti

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

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

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

$$\pi = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix}, \\ e = \begin{pmatrix} 4 & 5 & 6 & 2 & 3 & 1 \\ 4 & 6 & 5 & 3 & 1 & 2 \end{pmatrix};$$

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).⁹ Na př. je-li

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

a

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

⁹ Kdybychom se této nesrovnalosti chtěli vyhnout, museli bychom psát permutované číslo před permutací, tedy $(i)\pi$, místo $\pi(i)$, což by bylo méně vhodné.

pak

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

Nyní si dokažme, že *permutace stupně n tvoří vzhledem k uvedenému násobení grupu, t. zv. symetrickou grupu \mathfrak{S}_n , která je řádu $n! = 1 \cdot 2 \cdot 3 \dots n$.*

(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 t. zv. identickou permutací (čti jota)

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

(4) Axiom inverzního prvku je splněn, neboť zřejmě inverzní 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 $n! = 1 \cdot 2 \cdot 3 \dots n$ (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 theoreticky 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 t. zv. *Galoisově*¹⁰ teorii rovnic najde čtenář zmínku ve Schwarzově knížce „O rovnicích“, v této sbírce „Cesta k vědění“; pro základní pojmy Galoisovy theorie viz na př. Kurošovu učebnici.)

¹⁰ J. E. Galois, který předčasně zahynul v souboji, byl geniálním francouzským matematikem z počátku XIX. stol. (Zemřel ve věku 21 let.)

V theoretické fyzice nalézáme aplikace teorie symetrické grupy v kvantové mechanice,¹¹ kde jde o permutace elektronů v atomu či molekule.

Příklad 2. Grupa geometrických transformací.

Pro geometrii (i fyziku) je zásadně důležitý pojem *grupy geometrických* (po př. fyzikálních) *pohybů* čili transformací.¹² Tento pojem si objasníme na příkladě ze školy známých *euklidovských pohybů roviny*.

Představme si, že se tuhá rovina, unášející souřadnicový kříž x 0 y , pohnula v sobě samé, t. j. aniž se kterýkoli bod této roviny dostal mimo ni. Pak změnu polohy (pohyb) této roviny budeme posuzovat vzhledem k výchozímu postavení souřadnicového kříže. Bod, který měl *původně* úsečku hodnoty řekněme x' a pořadnici hodnoty řekněme y' (jež se po pohybu objevují a odečítají v *nové* poloze souřadnicového kříže), dospěl do místa bodu, jehož úsečka obnáší x a jehož pořadnice obnáší y (obojí měřeno v původní poloze souřadnicového kříže). „Nové“ souřadnice bodu x, y lze vyjádřit „starými“ souřadnicemi x', y' ze školy známými t. zv. transformáčními vzorci

$$\begin{aligned}x &= x' \cos \alpha - y' \sin \alpha + a, \\y &= x' \sin \alpha + y' \cos \alpha + b,\end{aligned}$$

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

Tyto *závislosti* nových souřadnic na starých (které ve svém úhrnu označme $T(\alpha, a, b)$), popisují a definují t. zv. *euklidovskou transformaci*, čili *euklidovský pohyb roviny*. Každý *euklidovský pohyb* T je plně určen uspořáda-

¹¹ Viz na př. B. L. van der Waerden, *Gruppentheoretische Methode in der Quantenmechanik*.

¹² Srov. s vysvětlením geometrického rázu pojmu pohybu *drobným tiskem* v odst. 1,1.

nou trojicí čísel α, a, b — t. zv. svými parametry. Způsob, jakým si označíme (staré či nové) souřadnice je lhostejný, je potřeba 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 vypíšeme takto:

$$\begin{aligned}x' &= x'' \cos \alpha' - y'' \sin \alpha' + a', \\y' &= x'' \sin \alpha' + y'' \cos \alpha' + b'.\end{aligned}$$

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

$$\begin{aligned}x &= (x'' \cos \alpha' - y'' \sin \alpha' + a') \cos \alpha - (x'' \sin \alpha' + y'' \cos \alpha' + \\ &+ b') \sin \alpha + a = x''(\cos \alpha' \cos \alpha - \sin \alpha' \sin \alpha) - y''(\sin \alpha' \cdot \\ &\cdot \cos \alpha + \cos \alpha' \sin \alpha) + a' \cos \alpha - b' \sin \alpha + a = x'' \cos(\alpha' + \\ &+ \alpha) - y'' \sin(\alpha' + \alpha) + a' \cos \alpha - b' \sin \alpha + b.\end{aligned}$$

Podobně

$$\begin{aligned}y &= x'' \sin(\alpha' + \alpha) + y'' \cos(\alpha' + \alpha) + a' \sin \alpha + \\ &+ b' \cos \alpha + b,\end{aligned}$$

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

$$\begin{aligned}a'' &= a' \cos \alpha - b' \sin \alpha + a, \\ b'' &= a' \sin \alpha + b' \cos \alpha + b.\end{aligned}$$

(Počátek se prvním pohybem T' , dostal do bodu a', b' a tento bod dostal se dalším pohybem T do bodu a'', b'').¹³

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 skládaných pohybů od prava doleva; hlubším důvodem pro toto nezvyklé psaní je okolnost, že zobecnění pojmu permutace na nekonečné soubory předmětů, jako jsou na př. body roviny, zahrnuje v sobě i pojem geometrické (euklidovské) transformace roviny jako zvláštní případ. Permutovanými předměty jsou pak na místě celých čísel páry reálných čísel (kde první číslo je úsečkou, druhé pořadnicí bodu) a euklidovský pohyb jakožto předepsané nahrazení starých souřadnic bodu, t. j. páru x', y' novými souřadnicemi téhož bodu, t. j. párem 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,¹⁴ že euklidovské pohyby možno považovat za prvky grupy, že totiž platí i pro skládání euklidovských pohybů, považované za „násobení“, v t. zv. *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

¹³ Na střední škole se při geometrickém odvozování součtové poučky pro \sin a \cos (jíž jsme tu užili při odvození parametrů výsledného pohybu) vychází 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 .

¹⁴ Přenechávám to čtenářově péli; asociativní zákon se nejlépe bez počítání dokazuje na základě předchozí poznámky, že pohyb roviny je permutace jejích bodů. (Asociativní zákon pro konečné permutace známe.)

ta grupa (t. zv. lineárních transformací či permutací) bodů¹⁵ roviny, která zachovává vzdálenost dvou bodů, což vychází na 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 tak, že

$$V = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} = \sqrt{(x'_1 - x'_2)^2 + (y'_1 - y'_2)^2}.$$

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, t. zv. neeuklidovských „pohybů“ roviny, odpovídajících „нееuklidovské“ geometrii. Důležitost theorie 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 theorie grup transformací s daným invariantem na tomto příkladě: Z požadavku speciální theorie 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 (neměnnosti) 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 (нееuklidovských) transformací, t. zv. grupa *Lorentzova*. Její studium je matematickým základem speciální theorie relativity.¹⁶ (Viz cvič. 10 k par. 1,4.)

Příklad 3. Grupa lineárních homogenních transformací (grupa matic).

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

¹⁵ 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.)

¹⁶ Čtenář se může poučit o theorii relativity v přístupně psané knížce *Fr. Závíšky*, nezapomenutelného profesora theoretické fyziky na KU, umučeného nacisty. Knížka má název „*Einsteinův princip relativity a theorie gravitační*“, vyd. JČMF.

homogenní transformaci, kdežto označení proměnných (nikoli jejich pořadí) je lhostejné. V dalším se omezíme na lineární homogenní transformace, kde je též počet závislých i nezávislých proměnných, tedy kde $m = n$ a dále takových, že z předpokládaných hodnot závisle proměnných x_1, x_2, \dots, x_n lze k nim vypočíst (jednoznačně) hodnoty závisle proměnných, t. j. řešit transformační rovnice podle neznámých x'_1, x'_2, \dots, x'_n . (Některý čtenář ví, že nutná a postačující podmínka takové řešitelnosti transformačních rovnic A je ta, aby t. zv. determinant soustavy byl číslem od nuly různým.¹⁸)

Neznámé x'_1, x'_2, \dots, x'_n lze tedy vyjádřit lineární homogenní závislostí na daných hodnotách x_1, x_2, \dots, x_n , čili lze nalézt t. zv. inverzní (lineární homogenní) transformaci. Máme tedy na mysli jen lineární homogenní transformace, které mají k sobě (lineární homogenní) transformaci inverzní.

Podobně jako při geometrických transformacích (příklad 2) budeme definovat i skládání lin. hom. transformací (též počtu proměnných) jejich postupným prováděním. Předvedeme si to na příkladě $n = 3$. Mějme dvě takové lin. hom. transformace.¹⁹

$$A = \begin{cases} x_1 = a_{11}x'_1 + a_{12}x'_2 + a_{13}x'_3 \\ x_2 = a_{21}x'_1 + a_{22}x'_2 + a_{23}x'_3 \\ x_3 = a_{31}x'_1 + a_{32}x'_2 + a_{33}x'_3 \end{cases}$$

$$B = \begin{cases} x'_1 = b_{11}x''_1 + b_{12}x''_2 + b_{13}x''_3 \\ x'_2 = b_{21}x''_1 + b_{22}x''_2 + b_{23}x''_3 \\ x'_3 = b_{31}x''_1 + b_{32}x''_2 + b_{33}x''_3 \end{cases}$$

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

¹⁸ O determinantech se čtenář poučí v každé základní učebnici (klasičké) algebry, anebo přímo v učebnici B. Bydžovského: Úvod do theorie determinantů a matic, JČMF Praha.

¹⁹ Číselné příklady najde čtenář níže — zde by však pravidelnost skládání transformací spíše zatemnil, než objasnil.

do rovnic pro A . Po příslušné úpravě vytyčáním dostáváme (provedení přenecháváme čtenáři jako snadné cvičení):

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

Součin AB obou lin. hom. transformací je tedy opět lin. hom. 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 inverzní (ln. hom.) transformaci, tvoří grupu, t. zv. homogenní *lineární grupu n -tého stupně*; při tom však je třeba ještě udat druh koeficientů, které vystupují v transformacích grupy, t. j. 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, viz literaturu na konci.)

Protože, jak jsme již zdůraznili, lin. 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 vynecháváme a mluvíme prostě o regulárních maticích stupně n ; slovo regulární (pravidelný) vyznačuje právě onu předpokládanou vlastnost příslušné lin. hom. transformace, že k ní existuje transformace inverzní (dle poznámky shora 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

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

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

Mezi maticemi (jakožto čtvercovými schematy 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 t. zv. 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

$$x_1 = x'_1, x_2 = x'_2, \dots, x_n = x'_n.$$

(Z definice násobení matic snadno vidět, že násobení jednotkovou maticí danou maticí 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 $b_{11} = b$ a pod.) Násobení matic je prostě násobení čísel. Příslušné homogenní transformace jsou ty nejjednodušší lineární závislosti, řekněme

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

a pod.

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

b) Položme $n = 2$. Nechť na př.

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

Pak

$$AB = \begin{pmatrix} 1 \cdot \frac{1}{2} + 2 \cdot 1 & 1 \cdot 0 + 2 \cdot 2 \\ 3 \cdot \frac{1}{2} + 4 \cdot 1 & 3 \cdot 0 + 4 \cdot 2 \end{pmatrix} = \begin{pmatrix} \frac{5}{2} & 4 \\ \frac{11}{2} & 8 \end{pmatrix}.$$

Matice AB přísluší k součinu (složení lin. hom. transformace)

$$\begin{aligned} x_1 &= x'_1 + 2x'_2 \\ x_2 &= 3x'_1 + 4x'_2 \end{aligned}$$

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

$$\begin{aligned} x &= \frac{1}{2}x', \\ y &= x' + 2y'. \end{aligned}$$

c) Hledejme inverzní matici k matici

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

Máme tedy nalézt matici X tak, aby

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

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 (inversní 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 transformace 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 theorie determinantů to ví předem, neboť si všimne, že determinant dané matice A je nula, protože druhý řádek matice je -2-kráté 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, t. j. hledme vypočíst hodnoty čárkovaných proměnných pomocí nečárkovaných z rovnic

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

Řešení je, jak se čtenář snadno přesvědčí

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

Tedy inverzní 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

$$\begin{aligned}BB^{-1} &= \begin{pmatrix} 1 \cdot 1 + 0 \cdot -\frac{1}{2} + 0 \cdot -\frac{1}{3} & 1 \cdot 0 + 0 \cdot 0 + 0 \cdot \frac{1}{3} \\ 1 \cdot 1 + 0 \cdot -\frac{1}{2} + 3 \cdot -\frac{1}{3} & 1 \cdot 0 + 0 \cdot 0 + 3 \cdot \frac{1}{3} \\ 1 \cdot 1 + 2 \cdot -\frac{1}{2} + 0 \cdot -\frac{1}{3} & 1 \cdot 0 + 2 \cdot 0 + 0 \cdot \frac{1}{3} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 + 0 \cdot \frac{1}{2} + 3 \cdot 0 \\ 1 & 0 + 2 \cdot \frac{1}{2} + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\end{aligned}$$

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

Příklad 4. Grupa idealisovaných 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, t. j. modř M , červeně \check{C} a žlutě \check{Z} 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 (theoreticky) docílit všech barevných odstínů jen tehdy, když jsou základní intensity modré, červené a žluté dosti jemné. Mísení barev, ovšem v příslušné idealisaci, podléhá zákonům komu-

tativní grupy, v níž neutrální barva N je jednotkovým prvkem a doplňková barva je prvkem inverzním. Tak na př. můžeme psát $M \cdot \check{C} \cdot \check{Z} = N$ čili $\check{Z}^{-1} = M \cdot \check{C}$ (t. j. doplňková barva ke žluti je „součin“ $M \cdot \check{C}$, což je fialová barva v základní síle). $\check{C}^2 \cdot \check{Z}$ je oranžová červenavého odstínu, $M^5 \cdot \check{C}$ je modř se slabě fialovým nádechem (při čemž čtenář vidí že symbolika theorie grup je s to vyjádřit barevné odstíny mnohem přesněji, než obvyklá názvosloví nauky o barvách).

Příklad 5. Booleova grupa.

Mějme jakýkoli počet předmětů, na př. 4 předměty, nazvané a, b, c, d . Utvořme z nich všechny skupiny (kombinace) bez ohledu na pořadí; těch je $2^4 = 16$, jestliže počítáme i t. zv. skupinu prázdnou, neobsahující žádný předmět, kterou označujeme jako \emptyset a t. zv. skupinu plnou, obsahující všechny předměty. Těchto 16 skupin budeme považovat za prvky jisté grupy, ve smyslu následujícího „násobení“: Za součin $X \cdot Y$ dvou skupin X a Y budeme považovat skupinu, která vznikne shrnutím předmětů z obou skupin X i Y a vyloučením předmětů, které jsou současně v obou skupinách. Tak na př. jestliže X se skládá z předmětů b, c, d a Y z předmětů a, b, c , pak $X \cdot Y$ se skládá z předmětů a, d . Když by Y bylo c, d pak $X \cdot Y$ bylo b .

Axiomy theorie grup jsou tu splněny (jak se laskavě čtenář sám může přesvědčit; větší námahu mu dá jen ověření platnosti axiomu asociativnosti). Jednotkovým prvkem je prázdná skupina \emptyset , inverzní skupinou ke skupině X je tato skupina sama, je $X^{-1} = X$, neboť platí (podle definice násobení v naší grupě) $X \cdot X = X^2 = \emptyset$ pro každou skupinu 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*²⁰ grupa.

²⁰ G. Boole byl anglický matematik z poloviny XIX. stol., který

Cvičení k 1,3.

1. Upravte na „normální tvar“

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

permutace

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

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

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

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 následovaným otočením o -60° .

5. Řešte v grupě euklidovských pohybů roviny rovnici

$$T(30^\circ; 1, 2) X = T(-90^\circ; -2, 5)$$

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.

vedle základních prací o t. zv. diferencním počtu proslul zavedením algebraického způsobu uvažování do theoretické logiky, čímž se stal jedním ze zakladatelů moderní matematické logiky.

8.*Ukažte, že následující násobení je grupové (jsou splněny axiomy 1, 2, 3, 4): Prvky grupy necht' jsou všechny skupiny předmětů, vybrané z n daných předmětů, včetně skupiny prázdné a skupiny všech n předmětů. Násobení necht' je dáno tímto předpisem: z daných dvou skupin — činitelů — utvoříme novou skupinu — součin — tím, že shrneme do jedné skupiny ty předměty, jež jsou současně v obou daných skupinách s těmi předměty, jež jsou současně mimo obě dané skupiny. (Jednotkou bude plná skupina.)

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 x .)

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

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

kde c je konstanta, v je parametr, $|v| \leq |c|$ tvoří grupu, t. zv. Lorentzovu grupu speciální teorie relativity. ($c \doteq 3 \cdot 10^{10}$ 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 .²¹

1.4. POJEM ISOMORFISMU GRUP. ABSTRAKTNÍ POJETÍ GRUPY (TYP ISOMORFISMU).

Jak jsme v předchozím poznali, prvky grupy mohou být věci velmi rozmanitého druhu: na př. zákrytové pohyby, čísla, permutace, geometrické transformace, matice, barvy, skupiny z daných předmětů. Násobení v grupě může být dáno velmi různými způsoby: na př. skládáním zákrytových pohybů, násobením čísel v původním smyslu slova, sečítáním čísel, kombinováním permutací v daném pořadí, postupným prováděním geometrických transformací, násobením

²¹ Srov. F. Závíska, *Einsteinův princip relativity a teorie gravitace*, JČMF Praha 1925, str. 60.