O grupách

ŠKOLA MLADÝCH MATEMATIKŮ

o grupách

LADISLAV RIEGER

PRAHA 1974
VYDAL ÚV MATEMATICKÉ OLYMPIÁDY
V NAKLADATELSTVÍ MLADÁ FRONTA

Recenzoval dr. Jiří Sedláček, CSc.
Část svazku Ladislava Riegera „O grupách a svazech“
pro I. vydání v edici Škola mladých matematiků
upravil doc. dr. Jaroslav Blažek, CSc.

KDO BYL
DOC. DR. LADISLAV RIEGER

Narodil se 25. června 1916 ve švédském Malmö a své mládí prožil v Roztokách, v Žilině a v Praze. Před druhou světovou válkou začal studovat matematiku a fyziku na Karlově universitě a po válečném přerušení dokončil studia doktorátem přírodních věd r. 1946. Jeho disertační práce byla r. 1948 poctěna cenou Královské české společnosti nauk. Od r. 1951 byl docentem matematiky na Českém vysokém učení technickém, odtud r. 1958 přešel do Matematického ústavu ČSAV v Praze. Rok poté dosáhl hodnosti doktora fyzikálně-matematických věd. Jeho vědeckým oborem byly speciální Booleovy a jiné abstraktní algebry a pak Gödelova axiomatika nekonečných i konečných množin spolu se speciálními aritmetikami. V širší veřejnosti se Rieger stal známým svou populární knížkou „O grupách a svazech", jež vyšla r. 1952 a z níž vznikl i tento nový svazek naší edice. Nemoc zastihla doc. dr. L. Riegera neočekávaně v době, kdy usilovně pracoval a měl ještě mnoho plánů. Zemřel v Praze 14. února 1963.

PŘEDMLUVA

Při sepisování populárně vědeckých knížek je vždy problém, jak spojit požadavek přístupného, a přitom stručného výkladu s požadavkem neúplatné věcné správnosti a matematické přesnosti. V abstraktním předmětu, jakým se obírá tato knížka, je tato potíž větší než jinde, a to tím spíše, že jde o látku jen zčásti zpracovanou v učebnicích teorie grup a vůbec ne, pokud je mi známo, v dobrých popularizujících publikacích. Do jaké míry se mi podařilo se s tímto problémem vyrovnat, to posoudí čtenáři.

V podstatě mi šlo o to seznámit čtenáře s některými základními pojmy teorie grup, která má v současné matematice základní význam. Chci ukázat na různorodém příkladovém materiálu, že běží o velmi obecnou matematickou zákonitost, kterou jsme objevili v nejrůznějších jejích konkrétních tvarech, v matematice i přímo ve skutečnosti.

Tato knížka nemá být učebnicí ani její náhražkou. Při jejím malém rozsahu a při daných předpokladech vědomostí nebylo samozřejmě možno probrat všechny základní pojmy — a ani o to nešlo. Šlo jen o to, aby si čtenáři odnesli z této knížky alespoň přesvědčení, že ani abstraktní algebraická teorie, jakou je teorie grup, není jen samoúčelná hříčka zasvěcených matematiků.

Kniha není určena pro odborníky; může je však přece

jen zajímat stať o induktivním důkazu jednoduchosti alternující grupy stupně $\neq 4$.

Aby si čtenář mohl překontrolovat, že textu porozuměl a aby si prohloubil a doplnil výklad samostatným uvažováním, jsou k většině kapitol připojena cvičení. Méně snadná jsou opatřena hvězdičkou, případně zběžným návodem k řešení.

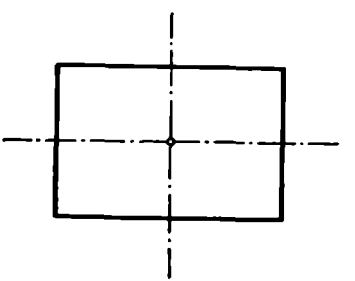
Ladislav Rieger

1. kapitola

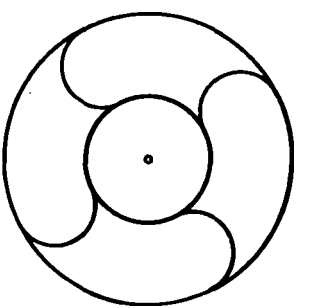
POJEM ZÁKRYTOVÉHO POHYBU

U čar a u plošných i prostorových útvarů, ať již vytvořených přírodou nebo lidmi, se setkáváme často s vlastností, které říkáme *geometrická pravidelnost*, ve zvláštním případě (středová, osová, rovinná) *souměrnost*. (Listy a květy rostlin, krystaly nerostů; ornamenty, stavby.)

V čem záleží (jak je definována) geometrická pravidelnost? Bez obšírných úvah lze říci, že útvar shledáváme geometricky pravidelným, jestliže lze udat tzv. *zákrytové pohyby*, jimiž se ztotožní útvar jako celek sám se sebou, při čemž se jeho jednotlivé body nemusí vrátit do svých původních poloh. Vystižení geometrické pravidelnosti útvaru je potřebí tedy hledat v množině jeho zákryto-



Obr. 1

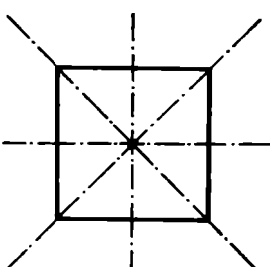


Obr. 2

vých pohybů. Tak např. obdélník (obr. 1) má tři takové zákrytové pohyby, tj. dvojí překlopení (dle každé z obou os souměrnosti) a jejich kombinaci, tj. otočení o 180°. Útvar na obr. 2 má rovněž přesně tři zákrytové pohyby, ale jiné, totiž otočení roviny o jeden, dva či tři pravé úhly. Nekonečný pás na obr. 3 má nekonečně mnoho

Obr. 3

zákrytových pohybů. Jsou to posuvy o celistvé násobky jednoho dílku pásu — a jiné zákrytové pohyby nemá. Čtverec (obr. 4) má 7 zákrytových pohybů (4 překlopení kolem os souměrnosti a 3 otočení o 90°, 180°, 270°).



Obr. 4

Aby později nevzniklo nedorozumění, je dobře výslovně objasnit geometrický ráz pojmu zákrytový pohyb. Na rozdíl od skutečného (fyzikálního) pohybu při zákrytovém pohybu nepřihlížíme ani k časovému

průběhu pohybu (k rychlosti), ani k tomu, po jaké dráze se jednotlivé body (geometricky pravidelného, tuhého) útvaru dostaly z původní do nové polohy. To znamená, že dva zákrytové pohyby platí za stejné, jestliže vedou z téže výchozí polohy útvaru do téže polohy konečné. Tak např. v obr. 2 otočení o úhel 90° a otočení o úhel 450° = 360° + 90° (v témže smyslu) považujeme za tentýž zákrytový pohyb. Pak je však důsledné připouštět za zákrytový pohyb i takový pohyb, při němž se každý jednotlivý bod vrátí odkud vyšel (ztotožní se se sebou samým). Takovému pohybu, danému např. otočením rovinného obrazce o 360°, říkáme pohyb identický, takže útvar na obr. 2 právě tak jako obdélník, mají ve skutečnosti po čtyřech zákrytových pohybech a při pásu na obr. 3 připouštíme i zákrytový posuv o nulovou délku. (Pak ovšem i geometricky zcela nepravidelné útvary mají zákrytový pohyb, totiž jediný, identický zákrytový pohyb.)

Množina zákrytových pohybů libovolného daného útvaru má některé důležité a jednoduché základní vlastnosti. Tak např. pozorujeme, že dva zákrytové pohyby provedeny po sobě (složeny) dají opět zákrytový pohyb, že ke každému zákrytovému pohybu existuje zákrytový pohyb zpětný, uvádějící útvar v každém jeho bodu do původní polohy (tedy skládající s daným pohybem pohyb identický) apod. Studium způsobů skládání zákrytových pohybů a těch souvislostí mezi těmito pohyby, které jsou skládáním dány (pouhý počet zákrytových pohybů říká příliš málo, jak jsme viděli na příkladě obdélníka a útvaru na obr. 1), tvoří matematický obsah teorie geometrické pravidelnosti. Tak jsme vedeni k pojmu grupy zákrytových pohybů, kterýmžto názvem označme prozatím zhruba množinu zákrytových pohybů daného útvaru spolu s předpisem, jak se

zákrytové pohyby skládají. Tento pojem si objasníme blíže pomocí příkladu zákrytových pohybů rovnostranného trojúhelníka.

Cvičení

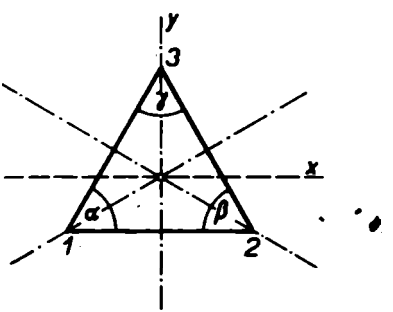
1. Určete zákrytové pohyby: a) pravidelného šestiúhelníka, b) vlnovky $y = \sin x$, c) neomezené čtvercové sítě v rovině, d) téže sítě opatřené ještě úhlopříčkami.

2. Ukažte, jak vynecháním a) vhodných bodů, b) vhodných úseček vznikne z rovnostranného trojúhelníka obr. 5) útvar o 3 zákrytových pohybech (kterých?).

2. kapitola

GRUPA ZÁKRYTOVÝCH POHYBŮ ROVNOSTRANNÉHO TROJÚHELNÍKA. AXIOMY GRUPY

Abychom mohli sledovat skládání zákrytových pohybů rovnostranného trojúhelníka (obr. 5)[1]) vyznačme si pro jednoduchost jednotlivé zákrytové pohyby takto: Písmena A, B, C nechť značí po řadě jednotlivá překlopení kolem osy úhlu α, β, γ. Písmena D a E nechť značí pohyby dané otočením roviny trojúhelníka o 120° a o 240° (proti směru ručiček hodin), a konečně J nechť značí identický pohyb (daný otočením o 0°). Tím jsme pojme-



Obr. 5

[1]) Čtenář učiní dobře, když si vystřihne z papíru rovnostranný trojúhelník (raději nikoli ten, který je na obr. 5 v knize) a sleduje názorně grupu jeho zákrytových pohybů podle dalšího výkladu; pozor na to, že po překlopení se mění smysl kladného otáčení.

novali všech 6 zákrytových pohybů rovnostranného trojúhelníka, jak se čtenář sám snadno přesvědčí. Smluvme si ještě (jednou provždy), že zákrytový pohyb, řekněme Z, vzniklý tím, že po jistém zákrytovém pohybu Y provedeme ještě jistý zákrytový pohyb X, budeme prostě psát jako XY, tedy $Z = XY$. Místo XX píšeme pak X^2. Skládání zákrytových pohybů rovnostranného trojúhelníka nyní nejlépe uvidíme na následující tabulce (tab. I), jejíž správné sestrojení nechť si čtenář ověří (viz pozn. 1).

Její užití je zřejmé: výsledek CD např. otočení o 120°, tj. pohybu D, následovaného překlopením kolem osy úhlu γ, tj. pohybem C, najdeme v průsečíku řádku uvedeného písmenem D a sloupce, uvedeného písmenem

	A	B	C	D	E	J
A	J	D	E	B	C	A
B	E	J	D	C	A	B
C	D	E	J	A	B	C
D	C	A	B	E	J	D
E	B	C	A	J	D	E
J	A	B	C	D	E	J

Tab. I

C, tedy odečteme $CD = B$ výsledek je překlopení kolem osy úhlu β; podobně $AB = E$, $AA = A^2 = J$ atp.

Pomocí tabulky I lze nyní pohodlně určovat i vý-

sledné zákrytové pohyby (rovnostranného trojúhelníka) složené předepsaným způsobem[2]) postupně z více než ze dvou pohybů.

$$(AB)\,C = EC = A,\ A^2D = D,\ (BC)\,(DE) = DJ = D$$

(Slovní význam těchto rovností si čtenář laskavě uvědomí sám.)

Již z toho, co bylo dosud řečeno a napsáno, čtenáře možná napadlo, že mezi skládáním zákrytových pohybů (v daném příkladě rovnostranného trojúhelníka) a násobením čísel je jistá podobnost. Vytkněme si, v čem skládání zákrytových pohybů (dejme tomu rovnostranného trojúhelníka) se shoduje s násobením čísel (mysleme pro určitost na kladná lomená — čili racionální — čísla), tj. formulujme zákony platné pro obojí. To jsou právě axiomy grupy.

Axiom (1)

Především nahlížíme, že libovolné dva zákrytové pohyby X a Y složeny v určitém pořadí X, Y dají opět zákrytový pohyb, řekněme $Z = XY$ (téhož rovnostranného trojúhelníka), při čemž výsledný zákrytový pohyb Z je určen jednoznačně, tj. nezávisle na tom, jakým způsobem byly provedeny pohyby X, resp. Y.

Podobně libovolná dvě kladná lomená čísla, řekněme $R = \frac{6}{5}$ a $S = \frac{1}{10}$, dají jednoznačně určený součin $RS = \frac{3}{25} = 0{,}12$ nezávisle na tom, zda číslo R je dáno

[2]) Zapisování po sobě následujících pohybů zprava doleva má svoje důvody, jež se objasní při definici „násobení" permutací a transformací ve 3. kap. Je důležité si na to zvyknout.

na příklad jako 1,2 nebo číslo S je dáno jako $\frac{4-2+3}{50}$ nebo jakkoli jinak — jen když jsou čísla táž.

Říkáme stručně, že skládání zákrytových pohybů, stejně jako násobení čísel, splňuje zákon neomezenosti a jednoznačnosti.

Axiom (2)

Dále shledáváme toto:

Skládáme-li jakékoli tři zákrytové pohyby Z, Y, X (v našem případě např. tři překlopení $X = A$, $Y = B$, $Z = C$), pak jsou dvě možnosti, jak to provést, aniž porušíme protiabecedně vyznačený sled kterýchkoli dvou z uvažovaných pohybů. Jednak lze nejprve utvořit pohyb YZ provedením pohybu Y po pohybu Z a nechat po již známém pohybu YZ následovat pohyb X. Za druhé možno pohyb Z nechat následovat (předem již známým) výsledkem XY složení pohybu Y následovaného pohybem X. Při prvé možnosti utvoříme tedy pohyb $X(YZ)$, při druhé pohyb $(XY)\,Z$. V našem příkladě máme jednou $A(BC) = AE = B$ a podruhé $(AB)\,C = EC = B$, tedy totéž. Snadno si uvědomíme, že tomu tak musí být při skládání pohybů vždycky, neboť i při druhé možnosti vlastně následují tři dané pohyby v daném pořadí právě tak jako při možnosti prvé.

Říkáme, že je splněn zákon asociativity a píšeme jej stručně

$$(XY)\,Z = X(YZ)$$

Tento zákon, jak dobře víme ze školy i z početní praxe, je splněn při násobení čísel (nahradíme-li zákryto-

vé pohyby čísly). Jeho důležitost (která bývá často stírána příliš povrchní formulací „nezáleží na uzávorkování") tkví v možnosti definovat jednoznačně složení tří (a více) zákrytových pohybů v daném pořádku rovnostmi

$$XYZ = (XY)\,Z = X(YZ)$$

z toho pak plyne možnost definovat

$$X^3 = XXX,\ X^4 = XXXX \text{ atd.}$$

Axiom (3)

Mezi čísly je právě jedno, totiž 1, nadáno vlastností, že nechává jakékoli číslo jím násobené beze změny. Tuto úlohu jednotky v souboru zákrytových pohybů má zmíněný identický zákrytový pohyb J, což zapisujeme rovnostmi

$$XJ = JX = X$$

platnými pro každý pohyb X. Říkáme, že je splněn zákon jednotkového prvku, pokud budeme později hovořit obecněji o prvcích grupy místo o zákrytových pohybech, budeme nazývat J jednotkovým prvkem.

Axiom (4)

Ke každému lomenému číslu L (rozumí se dle předpokladu $L > 0$) máme jedno jediné (kladné) číslo $\frac{1}{L}$, tzv. převrácenou hodnotu k L, tj. číslo, jež násobeno daným číslem dá jednotku, $L.\frac{1}{L} = 1 = \frac{1}{L}.L.$ (Píšeme raději L^{-1} namísto $\frac{1}{L}$.)

Podobně i ke každému zákrytovému pohybu (rovnostranného trojúhelníka) X máme přesně jeden zpětný pohyb X^{-1}, totiž takový, že po pohybu X se tímto pohybem X^{-1} vrátíme zpět do výchozí polohy, což píšeme rovností

$$X^{-1}X = J$$

Pohyby X a X^{-1} se vzájemně „ruší", tj. je též

$$XX^{-1} = J$$

Např. $A^{-1} = A$, protože $AA = A^2 = J$, nebo $D^{-1} = E$, protože $DD^{-1} = D^{-1}D = J = DE$. (Viz tabulka.)

Tomu, že ke každému zákrytovému pohybu existuje jeden jediný zpětný pohyb, říkáme, že je splněn zákon inversního prvku; ten dovoluje spolu se zákonem asociativity provádět u zákrytových pohybů obdobu dělení čísel, to jest: dovoluje ke dvěma daným pohybům Y a Z určit pohyb X tak, aby $XY = Z$; zřejmě totiž musí být $X = ZY^{-1}$. Podobně pro pohyb X hledaný rovnicí $YX = Z$ nalézáme $X = Y^{-1}Z$. Např. se ptejme, jaký pohyb musí předcházet před překlopením B kolem osy úhlu β našeho trojúhelníka, aby výsledek bylo otočení D o 120°? Nahlédnutím do tabulky zjišťujeme $X = B^{-1}D = BD = C$ jako odpověď, tj. jako řešení rovnosti $BX = D$. Slovy: hledaný pohyb je překlopení kolem osy úhlu γ.

Tuto důležitou okolnost, že zákrytové pohyby (rovnostranného trojúhelníka) splňují uvedené čtyři zákony (axiomy grupy) stručně vyjadřujeme rčením, že zákrytové pohyby tvoří grupu vzhledem k skládání pohybů. Čtyři axiomy grupy shrnují právě ty vlastnosti, jež splňuje každá množina všech zákrytových pohybů kteréhokoli geometricky pravidelného útvaru. Pojem grupy (zákrytových pohybů) tedy vystihuje

matematickou podstatu pojmu pravidelnosti útvarů (prostorových i rovinných). Viděli jsme však také, že grupové axiomy rovněž splňuje násobení (kladných lomených) čísel, kde tyto axiomy jsou ze školy nám dobře známými základními početními zákony, jichž užíváme v každodenní početní praxi, aniž jsme si toho pro jejich samozřejmost vědomi. Můžeme tedy říci, že kladná lomená čísla *tvoří vzhledem k násobení rovněž grupu*, tak zvanou multiplikativní grupu kladných lomených čísel.

Je však ještě jeden (početní) zákon (axiom), který je splněn pro násobení čísel a není splněn např. pro skládání zákrytových pohybů rovnostranného trojúhelníka, totiž tzv. zákon záměnnosti čili zákon komutativity.

Axiom (5)

Nezáleží na pořadí činitelů, stručně ve tvaru rovnosti

$$XY = YX$$

platné pro každé X a každé Y.

Skutečně totiž vidíme, že např. je

$$DA = C, \text{ ale } AD = B$$

slovy: překlopení kolem osy úhlu α následované otočením o 120° dá překlopení kolem osy úhlu γ, kdežto otočení o 120° následované překlopením kolem osy úhlu α dá překlopení kolem osy úhlu β.

Říkáme, že multiplikativní grupa kladných lomených čísel je *komutativní grupa*, také někde: *Abelova*[3]) grupa, kdežto grupa zákrytových pohybů rovnostranného trojúhelníka není komutativní.

[3]) Na počest předčasně zemřelého norského matematika N. H. Abela (1. pol. XIX. stol.).

Jsou tu ovšem i další rozdíly mezi oběma grupami. Tak například všech kladných lomených čísel je nekonečně mnoho, kdežto všech zákrytových pohybů rovnostranného trojúhelníka je konečně mnoho, totiž 6.

Říkáme, že multiplikativní grupa kladných lomených čísel je nekonečná, kdežto grupa zákrytových pohybů trojúhelníka rovnostranného je konečná, konečného řádu 6. Jiný rozdíl, souvisící s právě uvedeným, je tento: Libovolný zlomek a různý od jednotky má vesměs navzájem různé mocniny s celistvými kladnými mocniteli a, a^2, a^3, ... Naproti tomu libovolný zákrytový pohyb X trojúhelníka rovnostranného proveden šestkráte po sobě dá identický pohyb, tj. zde platí bez omezení rovnost $X^6 = J$, takže $X^7 = X$, $X^8 = X^2$, ... — „mocniny" se dále periodicky opakují. (Víme dokonce, že každý ze zákrytových — neidentických — pohybů rovnostranného trojúhelníka, poněvadž je to vždy buď překlopení, anebo otočení o 120°, resp. o 240°, splňuje vždy jednu z rovností $X^2 = J$ nebo $X^3 = J$.)

Za pomoci toho, co jsme právě uvedli, si tedy uvědomujeme tento souhrnný poznatek: *Některé* základní početní zákony, totiž tzv. zákony grupové (1) až (4), samozřejmě splněné při násobení (kladných lomených, případně i jiných) čísel nalézáme splněny i při skládání zákrytových pohybů geometricky pravidelných útvarů; tato okolnost, že zákrytové pohyby tvoří grupu, je společnou podstatou pojmu geometrické pravidelnosti. Skládáním zavádíme jakési „násobení" (ve zvl. př. „mocnění") zákrytových pohybů. Všechny vlastnosti, samozřejmé pro násobení a mocnění čísel však pro toto „násobení" již nejsou samozřejmými, zejména neplatí neomezený zákon záměnnosti pro skládání zákrytových pohybů.

K doplnění dodejme: Grupa zákrytových pohybů ne-

musí ovšem být konečná. Co více, z „konečnosti" pravidelného útvaru neplyne konečnost grupy zákrytových pohybů, jak to vidíme na zřejmě nekonečné grupě zákrytových pohybů kružnice. Rovněž z „nekonečnosti" (tj. neomezenosti) rovinného pravidelného útvaru neplyne nekonečnost grupy jeho zákrytových pohybů, jak to vidíme na grupě zákrytových pohybů obyčejného osového kříže (dvou navzájem kolmých přímek); tato grupa je řádu 8 (obsahuje 8 zákrytových pohybů: 4 překlopení a 4 otočení).

Uvedením do obecného pojmu grupy pomocí pojmu geometrické pravidelnosti sledujeme zhruba cestu, kterou (dle názoru některých matematiků) již staří Egypťané došli k neuvědomělé znalosti a použití tohoto jednoho ze základních pojmů moderní matematiky. Zároveň máme tak již na začátku možnost naznačit několik odpovědí na otázku, nač je teorie grup, tato základní disciplína abstraktní algebry. Bez obšírných výkladů je předně pochopitelné, že různé úlohy z ornamentální geometrické výzdoby (ať již plošné nebo prostorové) jsou v podstatě úlohami teorie grup zákrytových pohybů. Právě nepředstižné mistrovství starých Egypťanů v ornamentální geometricky pravidelné výzdobě je důvodem k názoru, že již oni v podstatě znali pojem konečné i nekonečné grupy, který se v novověké matematice objevuje teprve v XIX. století.

Teorie konečných grup (zákrytových pohybů) je dále podstatným pomocníkem nauky o tzv. pravidelných mnohostěnech vepsaných do koule.

Přímou praktickou důležitost má teorie grup zákrytových pohybů v krystalografii, tj. v nauce o geometrické pravidelnosti krystalů, ať již jde o tzv. makrokrystaly (viditelných rozměrů) nebo o mikrokrystaly (neviditelné pouhým okem).

Podobně má teorie grup aplikaci i v chemii, v teorii stereoisomerů, tj. v nauce o chemických sloučeninách týchž atomů v témž počtu, ale lišících se geometrickým uspořádáním v molekule.

Ve fyzice nalézáme aplikace teorie grup zejména v kvantové mechanice.

Cvičení

1. V grupě zákrytových pohybů rovnostranného trojúhelníka určete $ABCD = ?$, $ABDE = ?$, $A^2B^2 = ?$ Řešte rovnice $AX = E$; $XE = B$, $XB = X^2C$.

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

3. V grupě zákrytových pohybů rovnostranného trojúhelníka vypočtěte $A^{15} = ?$, $D^{-135} = ?$, $(AD)^{15} = ?$ (Návod: např. $D^3 = J = D^0$ apod.; užijte 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 $(XY)^n \neq X^nY^n$.)

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 otáčení roviny. Takové skládání splňuje 1., 3. a 4. axiom teorie grup, nikoli však 2. axiom asociativity. Přesvědčte se o tom.

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

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.]

4. kapitola

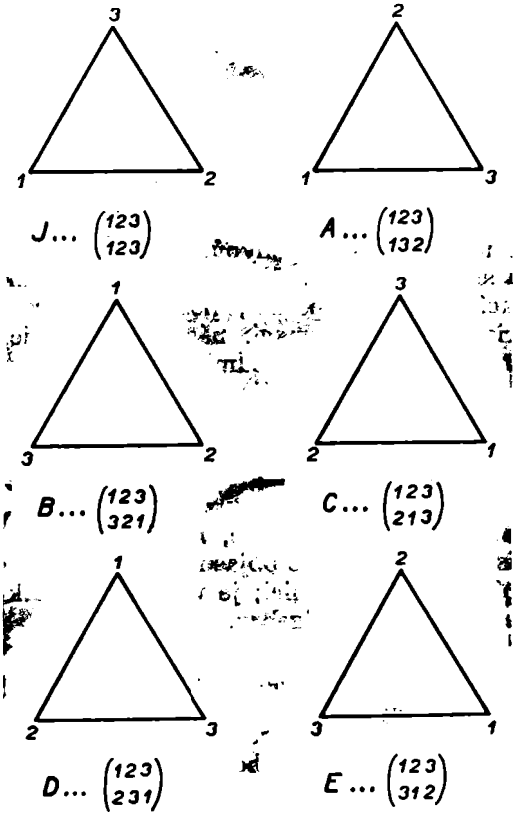
POJEM ISOMORFISMU GRUP. ABSTRAKTNÍ POJETÍ GRUPY (TYP ISOMORFISMU)

Jak jsme v předchozím poznali, prvky grupy mohou být věci velmi rozmanitého druhu: např. zákrytové pohyby, čísla, permutace, geometrické transformace, matice, barvy, skupiny z daných předmětů. Násobení v grupě může být dáno velmi různými způsoby: např. skládáním zákrytových pohybů, násobením čísel v původním smyslu slova, sečítáním čísel, kombinováním permutací v daném pořadí, postupným prováděním geometrických transformací, násobením matic, mísením barev, shrnováním předmětů ze dvou skupin do jedné, pokud se nevyskytují v obou.

Stává se však, že dvě grupy, ačkoli se liší vzájemně buď ve svých prvcích (některých či ve všech), anebo ve způsobu, resp. výsledcích grupového násobení, anebo v obojím, přece jsou *téhož typu*, čili, jak se říká, jsou *isomorfní* (z řec. iso = stejně, morfos = tvar). Pojem isomorfismu grup si dříve objasníme na příkladech, než přistoupíme k jeho definici; je to jeden ze základních pojmů celé abstraktní algebry.

Vraťme se ke grupě zákrytových pohybů rovnostranného trojúhelníka z 2. kap. Označme si jeho vrcholy v základní poloze číslicemi 1, 2, 3 od levého dolního vrcholu počínaje proti směru ruček hodin (obr. 5). Pak s každým zákrytovým pohybem dojde k určité současné náhradě každého z čísel 1, 2, 3 opět jedním z čísel 1, 2, 3, čili k permutaci čísel 1, 2, 3, nebo chceme-li, k permu-

taci vrcholů. Obráceně, každá ze šesti permutací tří čísel 1, 2, 3 je takto dána právě jedním zákrytovým pohybem našeho trojúhelníka. Avšak co je důležitějšího: zastoupíme-li jednotlivé zákrytové pohyby našeho



Obr. 6

trojúhelníka odpovídajícími permutacemi, pak jsme tím již zastoupili i každý součin (výsledek složení) pohybů součinem permutací, odpovídajících po řadě daným pohybům. Tak např. permutace $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ odpovídá překlopení A kolem osy úhlu α, permutace $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ odpovídá otočení E roviny trojúhelníka o 240°.

Součin obou permutací $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ je permutace odpovídající překlopení kolem osy úhlu β, $B = A.E$ (viz tab. v 2. kap. a obr. 6).

Vidíme tedy, že symetrickou grupu permutací S_3 můžeme od grupy zákrytových pohybů rovnostranného trojúhelníka odlišit jen konkrétní povahou prvků (jednou pohyby roviny trojúhelníka, podruhé permutace) a různým způsobem, jakým se provádí násobení. Pomocí vhodného vzájemně jednoznačného přiřazení prvků jedné grupy k prvkům druhé lze však přenést násobení z jedné grupy do druhé a obráceně.

Abychom náš příklad doplnili, sestrojme si ještě i grupu skládající se ze šesti dvojřádkových matic, která bude rovněž typu naší grupy všech permutací tří předmětů, čili typu grupy všech zákrytových pohybů rovnostranného trojúhelníka, a to pomocí příkladů 2 a 3 ze 3. kap.

Euklidovské otočení D roviny rovnostranného trojúhelníka o úhel 120° (čili o $\frac{2}{3}\pi$) je dáno lineární homogenní transformací

$$x = -\tfrac{1}{2}x' - \tfrac{1}{2}\sqrt{3}y'$$
$$y = \tfrac{1}{2}\sqrt{3}x' - \tfrac{1}{2}y'$$

protože

$$a_{11} = \cos\frac{2\pi}{3} = -\tfrac{1}{2}, a_{12} = -\sin\frac{2\pi}{3} = -\tfrac{1}{2}\sqrt{3},$$

$$a_{21} = \sin\frac{2\pi}{3} = \tfrac{1}{2}\sqrt{3}, a_{22} = \cos\frac{2\pi}{3} = -\tfrac{1}{2}$$

Podobně otočení $D^2 = E$ o 240° $\left(\text{čili o } \frac{4\pi}{3}\right)$ je dáno transformací

$$x = -\tfrac{1}{2}x' + \tfrac{1}{2}\sqrt{3}y'$$
$$y = -\tfrac{1}{2}\sqrt{3}x' - \tfrac{1}{2}y'$$

Konečně překlopení C kolem osy úhlu γ je dáno transformací

$$x = -x'$$
$$y = y'$$

Z obou otočení D a E a z překlopení C dovedeme složit všechny ostatní zákrytové pohyby rovnostranného trojúhelníka (viz tab. z 2. kap.), neboť nalézáme $A = CD$, $B = CE$. Nahraďme tedy zákrytové pohyby příslušnými, analyticky je vyjadřujícími lineárními homogenními transformacemi, skládání pohybů nahraďme postupným prováděním transformací a konečně transformace a jejich postupné provádění nahraďme příslušnými maticemi a jejich násobením podle předchozího odstavce. Dostaneme celkem toto vzájemně jednoznačné přiřazení zákrytových pohybů k permutacím a permutací k maticím 2. stupně (s reálnými koeficienty), které vzájemně přenáší skládání pohybů v násobení permutací a v násobení matic (srov. tab. I a obr. 6):

Zákrytový pohyb (rovnostr. trojúh.)	Permutace (3 vrcholů)	Matice (2. stupně)
Překlopení A (kolem osy úhlu α)	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}\frac{1}{2}&\frac{1}{2}\sqrt{3}\\\frac{1}{2}\sqrt{3}&-\frac{1}{2}\end{pmatrix}$
Překlopení B (kolem osy úhlu β)	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}\frac{1}{2}&-\frac{1}{2}\sqrt{3}\\-\frac{1}{2}\sqrt{3}&-\frac{1}{2}\end{pmatrix}$
Překlopení C (kolem osy úhlu γ)	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}-1&0\\0&1\end{pmatrix}$
Otočení D o $+120°$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}-\frac{1}{2}&-\frac{1}{2}\sqrt{3}\\\frac{1}{2}\sqrt{3}&-\frac{1}{2}\end{pmatrix}$
Otočení E o $+240°$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}-\frac{1}{2}&\frac{1}{2}\sqrt{3}\\-\frac{1}{2}\sqrt{3}&-\frac{1}{2}\end{pmatrix}$
Identický pohyb J	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$

Takovému vzájemně jednoznačnému přiřazení prvků jedné grupy k prvkům jiné grupy, jaké je tu vyznačeno, tedy takovému, které vystihuje násobení v jedné grupě násobením v jiné (které převádí násobení v jedné grupě v násobení v druhé), říkáme *isomorfní zobrazení* jedné grupy na druhou grupu; obě grupy pak platí za (vzájemně) isomorfní. Uveďme si ještě jeden každému dobře známý příklad takového isomorfního zobrazení jedné grupy na druhou. První grupa budiž *multiplikativní* grupa všech *kladných* reálných čísel, druhá grupa budiž *aditivní* grupa *všech* reálných čísel *vůbec*. Pak za isomorfní zobrazení první grupy na druhou můžeme považovat logaritmování (řekněme při základu 10). Ke každému kladnému číslu je dána jediná reálná hodnota jeho logaritmu při základu 10, každé reálné číslo (kladné, záporné i nula) je desítkovým logaritmem právě jednoho

kladného reálného čísla, a co hlavního, logaritmus součinu se rovná součtu logaritmů, čili násobení kladných reálných čísel se vystihuje (početně jednodušším) sečítáním čísel reálných (vůbec), totiž příslušných logaritmů. Z tohoto příkladu též vidíme, že takové isomorfní zobrazení jedné grupy (např. multiplikativní grupy kladných reálných čísel) na jinou grupu (např. aditivní grupu všech reálných čísel) nemusí být jen jedno, neboť právě takový isomorfismus dává i logaritmování při jiném, třeba při tzv. přirozeném základu.

Přistupme nyní k obšírné a přesné definici důležitého pojmu isomorfního zobrazení a isomorfismu grup.

Definice

Buďtež G a H dvě grupy. Nechť ke každému prvku x z grupy G je přiřazením f dán přesně jeden prvek $y = f(x)$ z grupy H, tzv. obraz prvku x z G při zobrazení f, tak, že jsou splněny tyto dvě podmínky:

(i) ke každému prvku y z grupy H existuje právě jeden prvek x z grupy G tak, že $y = f(x)$,

(ii) pro každé dva prvky x_1 a x_2 z grupy G je splněna rovnost

$$f(x_1x_2) = f(x_1).f(x_2)$$

(jestliže součin v G vyznačujeme prostým psaním činitelů vedle sebe a součin v H kvůli rozlišení vyznačujeme tečkou mezi činiteli). Pak zobrazení f se nazývá isomorfní zobrazení grupy G na grupu H.

Říkáme, že grupa G_1 je isomorfní s grupou G_2 jestliže existuje aspoň jedno takové isomorfní zobrazení G_1 na G_2, a vyznačujeme to symbolem

$$G_1 \cong G_2$$

V předchozím příkladě H byla multiplikativní grupa kladných reálných čísel, G byla aditivní grupa všech reálných čísel čili „.“ jest třeba nahradit „+“ (při čemž nic nevadí, že zde náhodou všechny prvky první grupy jsou obsaženy mezi prvky druhé grupy, což je ovšem možné jen při nekonečných grupách) isomorfní zobrazení f byl desítkový logaritmus, $f(x) = \log_{10} x$.

Jaký smysl má pojem isomorfismu grup?

Především ten, že stačí dokázat poučku o jedné určité grupě, abychom tím měli zároveň dáno neomezené množství odpovídajících pouček pro každou grupu, která se ukáže být s danou grupou isomorfní. Je to požadavek obecnosti výsledků teorie grup, který nutí k jasnému zavedení a využití pojmu isomorfismu.

Abstraktní teorie grup se tedy nezabývá určitou konkrétní grupou (jako např. je grupa permutací daného počtu předmětů nebo grupa matic s reálnými koeficienty daného stupně), nýbrž formuluje svoje poučky tak, aby platily pro všechny konkrétní, vzájemně isomorfní grupy současně, a to nejen pro ty, které již známe, nýbrž i pro všechny, s nimiž bychom se kdy mohli setkat. Čili abstraktní teorie grup má za své vlastní předměty celé typy vzájemně isomorfních grup (typy isomorfie, nebo jak se méně vhodně, ale stručněji říká, **abstraktní grupy**), nikoli jednotlivé grupy samotné. Abstrahuje se tu tedy jak od (početních) způsobů, jakými je v té které grupě vytváření součinu z jeho činitelů zavedeno (ať již si vzpomeneme např. na násobení permutací nebo násobení matic), tak i od samotného druhu prvků grupy (od toho, zda jsou to permutace nebo pohyby nebo i čísla.) Takováto abstrakce je právě nutná k tomu, abychom, přenášejíce vlastnosti a zákonitosti z jedné grupy na druhou (s touto isomorfní), nepřenesli případně omylem

nějakou specifickou vlastnost, založenou v povaze prvků nebo ve způsobu provádění násobení jedné konkrétní grupy, tedy vlastnost či vztah, které do vlastní teorie grup nepatří.

Pro typ isomorfismu grup je tedy podstatný 1. počet jejich prvků (v příslušném zobecnění i na tzv. nekonečný počet čili mohutnost množství prvků grupy), 2. okolnost, že ke každým dvěma prvkům grupy v daném pořadí je (nějak) stanoven jednoznačně jejich součin podrobený axiomům (1) až (4), lhostejno, jakým způsobem se násobení uskuteční.

Smysl popsané abstrakce v teorii grup je dále v tom, že abstraktní teorie grup, nepřestávajíc na abstraktním zevšeobecňování vlastností známých konkrétních grup systematicky hledá všechny typy grup, které jenom (popř. ještě za dodatečných předpokladů) jsou vůbec logicky možné, i když předem příklady takových grup známy nejsou; naopak, klade si, mimo jiné, za úkol takové příklady uměle hledat, sestrojovat je. Užitečnost takového počínání pro seznání grupové zákonitosti je právě taková, jako v přírodních vědách pokusné sestrojování přírodních dějů za umělých podmínek, které sice (popřípadě zatím) v přírodě nebyly nalezeny, ale mají pro poznání dané přírodní zákonitosti důležitý význam teoretický (jehož praktický dosah se musí dříve či později objevit).

Cvičení

1. Dokažte, že multiplikativní grupa všech komplexních čísel $\neq 0$ (tvaru $x + iy$) je isomorfní multiplikativní grupou matic tvaru

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \quad (x, y \text{ reálná čísla}, xy \neq 0)$$

2. Ukažte, že grupa zákrytových pohybů nekonečného pásu na obr. 3 je isomorfní s aditivní grupou celých čísel. (Udejte přesně isomorfní zobrazení.)

3. Ukažte, že grupa zákrytových otočení pravidelného n-úhelníka a multiplikativní grupa všech n-tých odmocnin z 1 jsou isomorfní grupy (cyklické grupy řádu n). (Udejte přesně isomorfní zobrazení.)

4. *Ukažte, že Booleova grupa ze 3. kap. a grupa ze cvič. 8* (za touž kap.) jsou isomorfní grupy (při stejném počtu daných předmětů). (Isomorfní zobrazení přiřazuje podmnožině předmětů jakožto prvku jedné grupy skupinu všech zbývajících předmětů (její doplněk) jakožto prvek druhé grupy.)

5. kapitola

GRUPOVÁ SCHÉMATA (TABULKY). ISOMORFNÍ REPREZENTACE LIBOVOLNÉ KONEČNÉ GRUPY GRUPOU PERMUTACÍ A GRUPOU MATIC

Zejména u konečných grup možno se při výzkumu a umělém sestrojování možných typů isomorfie grup (ve shora popsaném smyslu abstraktní teorie grup) opřít o zákonitosti ve čtverečném schématu z prvků grupy, jehož zápisem je grupová tabulka (jak jsme ji poznali již ve 2. kap., která právě dovoluje přehlédnout hotové výsledky grupového násobení bez ohledu na to, jak se k nim došlo. Uveďme si ještě jako čtyři příklady jednoduché grupové tabulky pro všechny grupy řádu 2, 3, 4 (*j* značí vždy jednotkový prvek, ostatní prvky jsou označeny malými latinskými písmeny).

	j	*a*
j	*j*	*a*
a	*a*	*j*

Tab. 2

	j	*a*	*b*
j	*j*	*a*	*b*
a	*a*	*b*	*j*
b	*b*	*j*	*a*

Tab. 3

	j	*a*	*b*	*c*
j	*j*	*a*	*b*	*c*
a	*a*	*b*	*c*	*j*
b	*b*	*c*	*j*	*a*
c	*c*	*j*	*a*	*b*

Tab. 4

	j	*a*	*b*	*c*
j	*j*	*a*	*b*	*c*
a	*a*	*j*	*c*	*b*
b	*b*	*c*	*j*	*a*
c	*c*	*b*	*a*	*j*

Tab. 5

Grupy v tab. 2, 3, 4 jsou tzv. cyklické grupy řádu 2, 3, 4. Obecně cyklickou grupou řádu n rozumíme grupu, jejíž všechny prvky se dají vytvořit mocninami svého vhodného prvku, řekněme a, např. a, $a^2 = j$ v tab. 2; a, $a^2 = b$, $a^3 = j$ v tab. 3; a, $a^2 = b$, $a^3 = c$, $a^4 = j$ v tab. 4. Obecně lze prvky cyklické grupy řádu n vypsat ve tvaru a, a^2, a^3, ..., a^{n-1}, $a^n = j$. (Název „cyklická" grupa pochází z faktu, že mocniny vytvářejícího prvku a se periodicky opakují: $a^{n+1} = a^n \cdot a = j \cdot a = a$, $a^{n+2} = a^2$, ..., což lze znázornit na kružnici.) Číselným případem cyklické grupy řádu n je multiplikativní grupa n-tých odmocnin z 1, což jsou ovšem obecně čísla komplexní.

Tabulka 5 předvádí tzv. Kleinovu grupu; je to komutativní grupa řádu 4, daná např. všemi zákrytovými pohyby obdélníka (nikoli čtverce).

Grupovou tabulku je vhodné zjednodušit tím, že na první místo úvodního řádku i sloupce dáme jednotkový prvek; pak úvodní řádek a úvodní sloupec můžeme vynechat, protože jeden i druhý se opakují v dalším řádku, resp. sloupci.

Jaké vlastnosti takového čtverečného schématu o n^2 polích obsazených n různými věcmi jsou typické pro grupová schémata? Odpověď, kterou podáme v následující větě, dává možnost studovat abstraktní typy isomorfismu konečných grup pomocí jisté konečné kombinatoriky čtverečných uspořádání n různých předmětů.

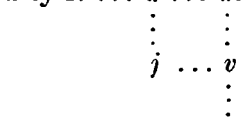
Věta 1

Čtvercové schéma o n^2 polích, zaplněných n různými předměty, j a, b, c, ... — při čemž předmět j nechť leží v levém horním rohu — představuje grupu s jednotkovým prvkem j (v našem smyslu, tj. tak, že za grupový součin xy libovolné-

ho předmětu x s libovolným předmětem y jest třeba pokládat předmět, který je v řádku, uvedeném předmětem x a ve sloupci, uvedeném předmětem y) tehdy a jen tehdy, splňuje-li takové schéma tyto dvě podmínky:

(1) *Každý předmět se vyskytuje v každém řádku a v každém sloupci (a tedy vždy jen jednou).*

(2) *Jestliže sloupec, v němž leží předmět u na místě k-tém shora, se protíná s řádkem, v němž leží předmět v na místě l-tém odleva, v poli obsazeném „jednotkou" j, potom řádek k-tý shora, se protíná se sloupcem l-tým zleva v poli, obsazeném součinem u.v).* (2) je tzv. obdélníkové pravidlo, znázorněné tímto výsekem z tabulky:



Důkaz: Tvrzení má dvě části. Jako první část dokažme, že jestliže předměty j, a, b, ... jsou prvky dané grupy, pak příslušné čtverečné schéma (znázorněné grupovou tabulkou „bez vstupů") má vlastnosti (1) a (2). Jako druhou část dokážeme, že obráceně má-li čtverečné schéma z předmětů j, a, b, ... vlastnosti (1) a (2), pak je tím dána určitá grupa s jednotkovým prvkem j.

Za prvé tedy nechť j je jednotkový prvek a a, b, c, ... ostatní prvky grupy, z nichž je tvořeno čtverečné schéma znázorněné tabulkou.

Vlastnost (1):

Kdyby se jistý prvek grupy, například a, vyskytoval v řádku, uvedeném třeba prvkem b dvakrát, jednou pod prvkem c a jednou pod prvkem d, pak by to znamenalo,

že $b.c = b.d$ $S=$ a. Z toho násobením prvkem b^{-1} zleva by vyplývalo $c = d$. Tedy skutečně nemůže být v témže řádku týž prvek dvakrát.

Vlastnost (2):

Podle předpokladu pro (2) mějme dva prvky u, v v naší grupě, které se vyskytují v příslušném grupovém čtverečném schématu v poloze, vyznačené nejlépe tímto výsekem z tabulky:

	c	...	d	
a	... u	...	ad	...
b	... j	...	v	...

To jest, vycházíme z rovností

$$a.c = u, \quad b.c = j, \quad b.d = v$$

a máme dokázat, že

$$a.d = u.v$$

Z napsaných rovností vyplývá pomocí asociativního zákona a pomocí zákona o inversním prvku

$$a.d = (u.c^{-1})\,(b^{-1}.v) = u(c^{-1}.b^{-1}).v = u.(b.c)^{-1}.v$$
$$= u.j^{-1}.v = u.j.v = u.v$$

protože je

$$(bc)^{-1} = c^{-1}b^{-1}, \text{ t.j. } (bc)\,(c^{-1}b^{-1}) = j$$

Za druhé, nechť čtverečné schéma splňuje podmínky (1) a (2). Máme dokázat, že násobení, zavedené ve smyslu, ve větě uvedeném, splňuje zákony grupy.

Zákon (1) neomezenosti a jednoznačnosti grupového součinu je splněn samozřejmě podle podmínky (1).

Zákon (2) asociativity snadno vyplývá z dvakráte užitého „obdélníkového pravidla", za pomoci tohoto výseku z tabulky:

$$\begin{array}{ccccc} u & \dots & uv & \dots & u(vt) = (uv)\,t \\ \vdots & & \vdots & & \vdots \\ j & \dots & v & \dots & vt \\ & & \vdots & & \vdots \\ & & j & \dots & t \end{array}$$

(Delší a nižší obdélník má v pravém horním rohu součin $u.(v.t)$ kratší a vyšší má na tomtéž místě součin $(u.v).t$; samozřejmě, že tvary obdélníků mohou být různé.)

Zákon (3) jednotkového prvku j je splněn samozřejmě přijatou úmluvou o tom, že první řádek a první sloupec schématu se setkávají v levém horním rohu v místě obsazeném předmětem j (vstupní řádek a vstupní sloupec je nyní nahrazen prvním řádkem a prvním sloupcem vlastní tabulky).

Rovněž konečně i zákon (3) inversního prvku je splněn, třebaže nikoli tak samozřejmě, jak by se snad mohlo zdát.

Abychom to dokázali, zaveďme si na chvíli toto označení: jestliže x je některý z našich n budoucích prvků grupy (tj. z předmětů vystupujících ve zkoumaném schématu), pak jako x_p^{-1} si označíme ten prvek, jímž je uveden sloupec, obsahující jednotkový prvek j v řádku, uvedeném prvkem x. Tento — podle předpokladu (1) — jednoznačně k libovolnému x určený prvek x_p^{-1} bychom mohli nazvat „pravým inversním prvkem" k prvku x, protože splňuje (dle toho, jak byl určen)

rovnost $x.x_p^{-1} = j$ (ve smyslu násobení daného pomocí naší tabulky). Podobně si jako x_L^{-1} označíme prvek, jímž je uvedena řádka, obsahující jednotku ve sloupci, uvedeném pod x. Prvek by mohl být nazván „levým inversním prvkem prvku x", protože splňuje rovnost $x_L^{-1}.x = j$. Nyní, užívajíce již dokázaného asociativního zákona pro naše násobení, máme vynásobením první rovnosti zleva prvkem x_L^{-1} a užitím druhé rovnosti

$$x_L^{-1}.(x.x_p^{-1}) = x_L^{-1}.j = x_L^{-1} = (x_L^{-1}.x).x_p^{-1} = x_p^{-1}$$

Je tedy $x_p^{-1} = x_L^{-1}$. Oba inversní prvky, pravý i levý jsou si rovny, existuje tedy právě jeden inversní prvek x^{-1} ke každému x. Tím je důkaz naší věty dokončen.

Praktické využití této věty k (více méně zkusmému) hledání všech možných typů konečných grup řádu n (při pevném n) sestrojováním tabulek, splňujících podmínky (1) a (2) věty, je velmi omezené: Již pro n, které překročilo 10, je sestavování grupových tabulek zdlouhavé a čím dále méně přehledné, pro náležitě veliké řády by pak nabývaly již samy tabulky (pokud písmena nemají se zmenšovat pod rozměry viditelné okem) nepraktických astronomických velikostí.

Je tedy třeba při studiu všech možných typů isomorfie grup, anebo jak se stručněji, ač méně správně říká, ke studiu abstraktních grup, užít jiných prostředků, totiž hlavně tzv. reprezentace abstraktních grup grupami permutací a grupami matic, o čemž bude řeč v následujícím. (Názvu „abstraktní grupa" možno užívat jen ve smyslu zkratky pro název „typ isomorfismu grup" — „abstraktní" grupy nejsou žádným zvláštním druhem grup.)

K pojmu isomorfní reprezentace abstraktní grupy grupou konkrétní, především grupou matic (jakožto grupou, v níž grupové násobení je dáno pomocí čtyř základních úkonů početních s čísly), jsme vedeni ještě i jinými důvody, z nichž uveďme alespoň tři.

Především všeobecně, jestliže jsme v pojmu typu isomorfismu grup dospěli na (ovšem relativní) vrchol abstrakce, potřebujeme také znát cestu dolů. Poněkud méně obrazně řečeno, jestliže v jistých úvahách teorie grup se nestaráme o to, jak v tom kterém případě se uskutečňuje grupové násobení (v tom či onom typu isomorfie grup), pak při jiných úvahách bychom naopak potřebovali vystihnout (abstraktně pojaté) grupové násobení násobením, které dobře známe z jistého druhu konkrétních grup; při tom musíme ovšem pro toto isomorfní uskutečnění a vystižení čili *reprezentaci* abstraktního grupového násobení konkrétním grupovým násobením zvolit takové reprezentující násobení, které je *univerzální*, aby každé grupové násobení se jím dalo vystihnout a za pomoci isomorfismu nahradit. Takovým univerzálním grupovým násobením je právě *násobení permutací* a ještě lépe: *násobení matic*. (Viz př. 1 a 3 ve **3. kap.**).

Druhým důvodem, který vlastně doplňuje a vysvětluje první, je opora, kterou nám v teorii grup poskytují vztahy mezi čísly, jestliže se nám podaří pomocí isomorfní representace nalézt ke každému typu isomorfismu (konečné nebo i nekonečné grupy, za zvl. předpokladů) grupu matic tohoto typu, jak jsme to například viděli v isomorfním vystižení grupy zákrytových pohybů rovnostranného trojúhelníka a zároveň symetrické grupy S_3 stupně 3 v předchozí kapitole.

Konečně třetí, ovšem nikoli nejméně důležitý důvod k hledání isomorfní reprezentace grup grupami matic,

jsou aplikace fyzikální a jiné, o nichž již byla zmínka.

Než se obrátíme k isomorfním reprezentacím, zaveďme si ještě další, v podstatě známý pojem.

Jestliže část prvků dané grupy tvoří (ve smyslu násobení v dané grupě zavedeného) sama pro sebe grupu, pak této grupě říkáme *podgrupa dané grupy*. Tak všechna celá čísla tvoří podgrupu aditivní grupy všech racionálních čísel (zlomků); tato grupa sama je podgrupou aditivní grupy všech reálných čísel (racionálních a iracionálních dohromady). Všechna čistá otočení, právě tak jako i všechny čisté posuvy tvoří dvě podgrupy v grupě všech euklidovských pohybů roviny. (Všimněme si, že obě podgrupy jsou komutativní, celá grupa však nikoli.) Všechny permutace z n prvních čísel tvoří podgrupu v grupě všech permutací jakéhokoli většího počtu m přirozených čísel.

Věta 2

Ke každé grupě G existuje s ní isomorfní podgrupa G' grupy všech permutací z tolika předmětů, kolik je prvků grupy G (čili jaký je v konečném případě řád n grupy G).

Důkaz: Za permutované předměty vezmeme pro zjednodušení přímo prvky dané grupy G. Samozřejmě že pomocí libovolného očíslování prvků grupy, pokud by jich ovšem byl jen konečný počet, můžeme převést permutace prvků dané grupy v permutace n přirozených čísel, což však již provádět nebudeme.

Ke každému pevnému prvku a z dané grupy G přiřaďme tu permutaci — označme ji π_a, která nahrazuje libovolný prvek x grupy G jeho levým a–násobkem $a.x$, tedy $\pi_a(x) = a.x$. Že π_a je skutečně permutace, je zřejmé, neboť současná náhrada všech prvků x prvky $a.x$ mění dva různé prvky x_1 a x_2 ve dva různé násobky

ax_1 a ax_2, protože by jinak z $a.x_1 = a.x_2$ vyplývalo $x_1 = x_2$ vynásobením prvkem a^{-1} zleva.

Že dvěma různým prvkům grupy a a b jsou takto přiřazeny dvě různé permutace, je rovněž zřejmé, neboť permutace π_a převádí prvek $x = j$ (jednotkový prvek) v prvek a, kdežto permutace π_b převádí týž prvek j v jiný prvek b. Je tedy přiřazení permutace π_a k prvku a grupy vždy vzájemně jednoznačné a zbývá, dle definice 1 ukázat, že součinu prvků je takto přiřazen součin permutací (ve smyslu př. 1, ze 3. kap.) přiřazených daným prvkům. Máme se tedy přesvědčit o platnosti rovnosti

$$\pi_a . \pi_b = \pi_{ab}.$$

Tato rovnost neříká nic jiného, než to, že znásobit libovolný prvek x naší grupy součinem $a.b$ zleva dá totéž, jako znásobit součin $b.x$ zleva prvkem a. To však je právě zaručeno asociativním zákonem. Tím je důkaz věty 2 proveden.

Věta 2 nám tedy zaručuje, že mezi podgrupami symetrické grupy všech permutací (dejme tomu pro konkrétnost) n prvních přirozených čísel nalezneme zástupce všech typů isomorfismu grup řádu n. (Poněvadž jsme však předpokladu konečnosti grupy G nikde v důkazu neužili, platí věta i pro nekonečné grupy, viz 4. kap.). Pozor na to, že symetrická grupa permutací n předmětů, která sama má $n!$ prvků, to jest permutací, může být tedy isomorfně reprezentována podgrupou v symetrické grupě všech permutací z $n!$ předmětů.

Obraťme se k maticím.

Věta 3

Budiž G libovolná grupa (nikoli nutně všech) permutací

z m předmětů (permutací stupně m). Pak existuje v grupě všech regulárních matic stupně m podgrupa isomorfní s danou grupou G.

Důkaz: Permutované předměty si nyní pro jednoduchost nahraďme přirozenými čísly 1, 2, 3, ..., m. (Všechny indexy i, k, l, r, s budou nabývat hodnot od 1 do m.)

Budiž π libovolná permutace z grupy G, která nechť převádí číslo i v číslo $\pi(i)$ (ovšem že $1 \leqq i \leqq m$). Přiřaďme této permutaci π m-řadovou čtverečnou matici, která má v i-tém řádku a v $\pi^{-1}(i)$-tém sloupci (kde π^{-1} je inversní permutace k permutaci π) číslo 1 a na všech ostatních místech má číslo 0, tj. k π přiřazujeme matici (a_{ik}), kde $a_{ik} = 1$ pro $k = \pi^{-1}(i)$ a $a_{ik} = 0$ pro $k \neq \pi^{-1}(i)$. Matice a_{ik} takto přiřazená k permutaci π je jistě regulární, neboť odpovídá lineární homogenní transformaci velmi prostého tvaru

$$\begin{aligned}
X_1 &= 0.X_1' + 0.X_2' + \ldots + 1.X_{\pi^{-1}(1)} + \ldots + 0.X_m' \\
X_2 &= 0.X_1' + 0.X_2' + \ldots + 1.X_{\pi^{-1}(2)} + \ldots + 0.X_m' \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_m &= 0.X_1' + 0.X_2' + \ldots + 1.X_{\pi^{-1}(m)} + \ldots + 0.X_m'
\end{aligned}$$

(Řešení napsaných transformačních rovnic dle čárkovaných neznámých je tím totiž napsáno; je třeba jen převrátit strany rovnic a vhodně přeměnit jejich pořadí; snadno nahlížíme, že lze psát řešení ve tvaru

$$\begin{aligned}
X_1' &= 0.X_1 + 0.X_2 + \ldots + 1.X_{\pi(1)} + \ldots + 0.X_m \\
X_2' &= 0.X_1 + 0.X_2 + \ldots + 1.X_{\pi(2)} + \ldots + 0.X_m \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_m' &= 0.X_1 + 0.X_2 + \ldots + 1.X_{\pi(m)} + \ldots + 0.X_m)
\end{aligned}$$

Protože provedené přiřazení matic k permutacím je zřejmě vzájemně jednoznačné, zbývá jen dokázat, že

součinu dvou permutací $\pi.\varrho$ je přiřazena matice, která je součinem matic, přiřazených k oběma permutacím, a to ve stejném pořadí činitelů. Nechť tedy první permutaci π je přiřazena matice (a_{ik}) s $a_{i\pi^{-1}} = 1$ a $a_{ik} = 0$ pro $k \neq \pi^{-1}(i)$ a podobně permutaci ϱ matice (b_{rs}) s $b_{r\varrho^{-1}} = 1$ a $b_{rs} = 0$ pro $s \neq \varrho^{-1}(r)$ $(i, k, r, s = 1, 2, 3, \ldots, m)$. Znásobením obou matic obdržíme (viz 4. kap.) dle definice

$$(a_{ik}).(b_{rs}) = (c_{is})$$

kde

$$c_{is} = a_{i1}b_{1s} + a_{i2}b_{2s} + \ldots + a_{im}b_{ms}$$

Jasné je, že koeficienty c_{is} matice, která je výsledkem provedeného násobení, budou opět jen čísla 0 nebo 1. Z uvedené definice násobení matic („řádka kráte sloupec") plyne, že bude $c_{is} = 1$ jedině tehdy, když v i-tém řádku matice (a_{ik}) je jednotka na tolikátém místě, na kolikátém (shora) je jednotka v s-tém sloupci matice (b_{rs}). V i-tém řádku matice (a_{ik}) je však vždy jednotka právě na místě $\pi^{-1}(i)$-tém. V s-tém sloupci matice (b_{rs}) je vždy jednotka na právě takovém místě k-tém (shora), že $\varrho^{-1}(k) = s$ čili $k = \varrho(s)$. Tedy k tomu, aby (součet ze součinů) c_{rs} při znásobení r-tého řádku první matice s s-tým sloupcem druhé byl roven 1, je nutno a stačí, aby $\pi^{-1}(r) = k = \varrho(s)$ čili aby $s = \varrho^{-1}\pi^{-1}(r)$. Pak tedy $c_{rs} = 1$ pro $s = \varrho^{-1}\pi^{-1}(r)$ a jinak $c_{rs} = 0$; protože však je $\varrho^{-1}\pi^{-1} = (\pi\varrho)^{-1}$, je tedy $s = (\pi\varrho^{-1}(r)$, takže skutečně obdržená matice c_{rs} je ta, která je přiřazena k permutaci $\pi.\varrho$, čímž je důkaz proveden.

Z věty 2 a 3 plyne ihned

Věta 4

Každá grupa řádu m je isomorfní s jistou grupou matic stupně m (m-řadových matic).

Dle věty 2 lze totiž každou grupu isomorfně reprezentovat vhodnou grupou permutací a dle věty 3 tuto grupu permutací lze opět isomorfně reprezentovat grupou matic; je tím tedy i dána isomorfní reprezentace dané grupy grupou matic.

Věty 3 a 4 mají spíše teoretický, než praktický význam: Zaručují hledanou univerzálnost násobení permutací a násobení matic a dávají nejjednodušší možnost každé grupové násobení v libovolné konečné (a ve vhodném zobecnění i nekonečné) grupě převést v násobení permutací a ještě lépe v násobení matic, to jest v násobení vykonávané pomocí sečítání, odčítání, násobení a dělení čísel. Avšak reprezentace ve smyslu věty 4 vede na matice zbytečně vysokého stupně, totiž rovného řádu grupy. Prakticky, pro studium struktury dané grupy, mají větší význam reprezentace maticemi co nejmenšího stupně (o co nejmenším počtu řádků), kde také větší rozmanitost číselných koeficientů matic a tedy i bohatost jejich vztahů dává více možností využívat aritmetických poznatků pro teorii grup. Prostý příklad takové úsporné a účinné reprezentace grupy zákrytových pohybů rovnostranného trojúhelníka, čili tím i symetrické grupy všech permutací stupně 3 (která je řádu 6), grupami matic stupně 2 jsme si probrali v předchozí kapitole.

V dalším opustíme pojem isomorfní reprezentace, abychom alespoň z dálky ukázali, jakým způsobem řeší abstraktní teorie grup řadu dalších svých typických úkolů. Jde o to, jakým způsobem jednoduché podmínky, kladené na blíže neurčenou grupu, omezují její možný

typ isomorfismu, s cílem stupňovat takové přehledné podmínky tak, až jsou jimi možnosti pro typy isomorfie grupy úplně a přehledně určeny. Poněkud obecněji řečeno, studium logických závislostí jedněch vlastností abstraktní grupy na jiných vlastnostech jiné nebo téže grupy je dalším hlavním úkolem tzv. obecné teorie grup.

Zvláště významný je jmenovitě úkol, na nějž se často v aplikacích teorie grup naráží (např. v aplikacích na teorii algebraických rovnic a na krystalografii), totiž získat co možno úplný přehled o počtu a souvislostech podgrup v grupě, podrobené určitým podmínkám; zvláště pak běží o tzv. normální podgrupy. Abychom mohli alespoň naznačit tyto problémy a jejich řešení, musíme se seznámit s několika dalšími základními, již abstraktními pojmy teorie grup.

Cvičení

1. Ukažte, že grupa je komutativní tehdy a jen tehdy, jestliže její tabulka je souměrná dle hlavní úhlopříčky (zleva nahoře dolů doprava).

2. *Přesvědčte se na podkladě úlohy 1, že všechny grupy řádu menšího než 6 jsou komutativní (Abelovy).

3. *Ukažte, jak je Kleinova grupa isomorfně reprezentována grupou matic

$$j = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

4. Přesvědčte se, že matice daného stupně n takové, že v libovolném řádku a v libovolném sloupci je jediné komplexní číslo různé od nuly — tvoří nekomutativní nekonečnou grupu, tzv. monomiální grupu stupně n. Tato grupa je isomorfní s grupou speciálních tzv. monomiálních (česky: jednočlenných) (lineárních homogenních) transformací tvaru

$$\begin{aligned} x_1' &= k_1 x_{\pi(1)} \\ x_2' &= k_2 x_{\pi(2)} \\ &\dots\dots\dots\dots \\ x_n' &= k_n x_{\pi(n)} \end{aligned}$$

($i = 1, 2, \dots, n$; $\pi(i)$ je permutace hodnot indexu i), $0 \neq k_i$ jsou komplexní čísla.

5. Přesvědčte se, že jestliže koeficienty $k_1, k_2, \dots, k_n$ probíhají pouze čísla z jisté podgrupy multiplikativní grupy komplexních čísel, pak dostaneme monomiální podgrupy monomiální (viz cvič. 4) grupy stupně n. Dokažte, že probíhají-li čísla k_i grupu řádu m, pak taková podgrupa monomiální grupy obsahuje $m^n n!$ prvků (matic).

6. Sestrojte tabulku monomiální (viz cvič. 4) podgrupy stupně 2 pro $k_{1,2} = \pm 1$.

7. Ukažte, že v monomiální (viz cvič. 4) podgrupě stupně 2, kde $k_{1,2}$ probíhají grupu všech 4-tých odmocnin z 1 (t. j. čísla $+1, -1, +i, -i$ ($i = \sqrt{-1}$)) tvoří následující matice podgrupu řádu 8

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm i & 0 \\ 0 & \pm i \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}$$

Ukažte, že v této podgrupě platí tyto vztahy: označíme-li

$$\pm \boldsymbol{i} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \pm \boldsymbol{j} = \begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix}, \pm \boldsymbol{k} = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix},$$
$$\boldsymbol{l} = \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}: \text{ pak je}$$
$$\boldsymbol{i}^2 = \boldsymbol{i}, \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{l}^2 = -\boldsymbol{i}, \boldsymbol{jk} = 1,$$
$$\boldsymbol{kj} = -1, \boldsymbol{kl} = \boldsymbol{j}, \boldsymbol{lh} = -\boldsymbol{j}, \boldsymbol{lj} = \boldsymbol{k}, \boldsymbol{jk} = -\boldsymbol{k}$$

Sestrojte tabulku: $+\boldsymbol{i}, +\boldsymbol{i}, +\boldsymbol{j}, +\boldsymbol{k}$ jsou tzv. základní Hamiltonovy kvaterniony.

8. Ukažte, že multiplikativní grupa všech komplexních čísel o absolutní hodnotě = 1 je isomorfní s grupou všech euklidovských otočení roviny (viz cvič. 1 ke 4 kap.).

9. *Ukažte, že všechny regulární lomené transformace $T(a_1, b_1, a_2, b_2)$ jedné reálné (popř. komplexní) proměnné x tvaru

$$T(a_1, b_1, a_2, b_2) = \left\{ x' = \frac{a_1 x + b_1}{a_2 x + b_2} \right.$$

kde a_1, b_1, a_2, b_2 jsou reálná (komplexní) čísla, tj. parametry transformace $T(a_1, b_1, a_2, b_2)$, která je jimi plně určena, a kde $a_1 b_2 - a_2 b_1 \neq 0$ (podmínka regulárnosti) tvoří grupu (zvláštní případ tzv. projektivní grupy).

Ukažte, že tato grupa (která jakožto grupa transformací jedné proměnné není lineární) je isomorfní s grupou všech lineárních homogenních transformací dvou proměnných (čili je isomorfní s grupou všech regulárních matic stupně 2).

Ukažte, že tzv. afinní transformace tvaru $x' = a_1 x + b_1$ tvoří podgrupu (zvl. případ tzv. afinní grupy).

6. kapitola

ROZDĚLENÍ PRVKŮ GRUPY DO TŘÍD DLE PODGRUPY. HOMOMORFNÍ ZOBRAZENÍ, NORMÁLNÍ PODGRUPA, FAKTOROVÁ GRUPA. 1. A 2. VĚTA O ISOMORFISMU. POJEM JEDNODUCHÉ GRUPY

Budiž G nějaká grupa a H nějaká její podgrupa. Vynásobme si libovolně zvoleným prvkem x grupy G postupně všechny prvky z podgrupy H zleva, tedy utvořme si všechny prvky tvaru $x.h$, kde h probíhá celou podgrupu H. Souhrn těchto prvků si označíme jako $x.H$ a nazýváme jej *levou třídou prvku x podle podgrupy H*.

Ukážeme si dva pozoruhodné fakty. Za prvé, pro prvky x_1 a x_2 jsou jen dvě možnosti: buďto obě třídy splývají (obsahují tytéž prvky grupy), anebo obě třídy nemají společné prvky. Jsou totiž jistě jen dva možné případy: buďto obě třídy x_1H a x_2H mají společný prvek, anebo společný prvek nemají. V prvním případě budiž x takový společný prvek. Potom je $x = x_1.h_1 = x_2.h_2$ při vhodných prvcích h_1 a h_2 z podgrupy H. Libovolný prvek z levé třídy x_1H má tvar $x_1.h$, kde h je prvek z podgrupy H. Dosazením z předchozího máme

$$x_1.h = x_2.h_2.h_1^{-1}.h$$

Protože H je podgrupa, leží v ní s prvky h_1, h_2, h i součin $h_2.h_1^{-1}.h$, takže libovolný prvek $x_1.h$ z levé třídy prvku x_1 patří do levé třídy prvku x_2. Právě tak dokážeme, že

i obráceně libovolný prvek z levé třídy prvku x_2 patří do levé třídy prvku x_1. Je tedy v případě společného prvku opravdu dokázáno, že obě levé třídy splývají, čímž je náš prvý fakt prokázán.

Druhý fakt vyslovíme jen pro konečné grupy, ačkoli v příslušném zobecnění pojmu počtu prvků na nekonečné souhrny (viz pozn. 3) platí rovněž. Zní takto: všechny levé třídy dle téže podgrupy obsahují týž počet prvků grupy, tak veliký, kolik je prvků podgrupy.

Libovolná levá třída xH obsahuje jistě nejvýše tolik prvků grupy, tj. násobků prvky z podgrupy H, kolik je v H prvků. Avšak žádné dva různé prvky h_1 a h_2 z podgrupy H nemohou dát vynásobením týž prvek levé třídy, protože z $x.h_1 = x.h_2$ by plynulo vynásobením prvkem x^{-1} zleva, že $h_1 = h_2$.

Oba poznatky spojeny tedy praví, že prvky grupy jsou každou její podgrupou rozděleny do jistého počtu „přihrádek", to jest levých tříd podle dané podgrupy, při čemž počet prvků ve třídě je týž pro každou z nich. Mezi levými třídami ovšem vystupuje i podgrupa sama jakožto třída jednotkového prvku grupy. Z toho máme tento důsledek:

Věta 5

V každé konečné grupě je řád (tj. počet prvků) grupy násobkem řádu každé z jejích podgrup.

Skutečně, řád podgrupy je tolikrát obsažen v řádu grupy, kolik je levých tříd dle této podgrupy. Výsledek dělení řádu grupy řádem podgrupy se nazývá *indexem* dané podgrupy.

Rozumí se, že podobné úvahy lze dělat právě tak pro podobně definované pravé třídy dle podgrupy, což si tu odpustíme.

Zvláště jednoduše tvořenými podgrupami, které nalézáme v každé grupě jsou tzv. *cyklické podgrupy*. Je-li G daná grupa a a její prvek, pak cyklická podgrupa je tvořena všemi mocninami prvku a

$$\ldots, a^{-2}, a^{-1}, a^0 = j, a^1, a^2, \ldots$$

Jestliže grupa G je konečná, nemohou být ani mocniny

$$a = a^1, a^2, a^3, \ldots$$

všechny různé, nýbrž musí být při jistém přirozeném mocniteli m větším než jiné přirozené k $a^m = a^k$, čili $a^{m-k} = j$; některé přirozené mocniny prvku a dávají jednotku (grupy) j. Nejmenší přirozený kladný mocnitel n, pro nějž je $a^n = j$, — existuje-li ovšem — je tzv. *řád prvku*. Je to zároveň i řád cyklické podgrupy, vytvořené prvkem a, protože prvky této cyklické podgrupy jsou mocniny $a, a^2, a^3, \ldots, a^{n-1}, a^n = j$ v počtu n. (Nepřekvapuje nás, že pak je třebas pro prvek a řádu 7

$$a^{-4} = a^3, a^9 = a^2)$$

Neexistuje-li takové n, aby $a^n = j$, pak říkáme, že prvek je nekonečného řádu. V tom případě jsou vesměs různé mocniny

$$\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = j, a^1, a^2, a^3, \ldots$$

a tvoří tzv. nekonečnou cyklickou grupu. Nekonečné cyklické grupy jsou zřejmě isomorfní s aditivní grupou všech celých čísel, totiž mocnitelů vytvářejícího prvku a. Berouce speciálně v úvahu cyklické podgrupy můžeme vyslovit tento *důsledek věty 5:*

Řád prvku konečné grupy je dělitelem řádu grupy.

Z tohoto tvrzení plyne tzv. malá Fermatova[18]) věta číselné teorie.

Malá Fermatova věta praví toto: Jestliže a je celé číslo nesoudělné s celým kladným číslem n, a jestliže označíme jako $\varphi(n)$ počet celých kladných čísel menších než n a nesoudělných s n (krátce nesoudělných zbytků)[19]) — číslo 1 v to počítaje — potom mocnina $a^{\varphi(n)}$ částečně vydělena číslem n zanechává zbytek 1. Krátce tvrzení vypisujeme symbolem

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

smluvivše si, že $x \equiv y \pmod{n}$ (čti: x kongruentní s y modulo n) znamená obecně, že rozdíl $x - y$ je násobkem celého kladného čísla, n tzv. modulu ($0 = 0.n$ je rovněž násobek čísla n). φ je tzv. *Eulerova*[20]) funkce číselné teorie.

Odvození malé Fermatovy věty z našeho důsledku věty 5 bude ukázkou aplikace abstraktní poučky z teorie grup na konkretním matematickém materiálu. Proveďme je proto důkladně.

Běží vlastně pouze o vytčení vhodné grupy tak, aby téměř bezprostředním užitím našeho tvrzení (že totiž řád prvku konečné grupy je dělitelem řádu grupy) na tuto grupu vyplynula malá Fermatova věta. K tomu cíli musíme učinit dvě věci: předně vytknout, co budou

[18]) Fermat byl veliký francouzský matematik ze 17. stol., jeden ze zakladatelů novověké matematiky. (Pojem grupy ovšem ještě neznal.)

[19]) $\varphi(1)$ definujeme rovno 1

[20]) L. Euler byl znamenitý německý matematik 18. stol., který prožil část života v Rusku v tehdejším Petrohradě (Leningradě).

prvky naší grupy, a za druhé určit pro ně grupové násobení.

Prvky naší grupy budou nikoli snad jednotlivá čísla, nýbrž jisté celé tzv. zbytkové třídy dle dělitele, tzv. modulu n, tj. budou to od sebe oddělené skupiny celých čísel a každá z těchto skupin bude obsahovat nekonečně mnoho celých čísel. Do jedné takové skupiny dáme všechna celá čísla, která dávají týž celý nezáporný zbytek při dělení modulem n. Jinými slovy, dvě celá čísla a a b patří do téže zbytkové třídy dle modulu n, což píšeme $a \equiv b \pmod{n}$, tehdy a jen tehdy, když rozdíl $a - b$ je dělitelný modulem n (slovem dělitelný rozumí se vždy dělitelný beze zbytku); totéž platí ovšem i o rozdílu $b - a = -(a - b)$. (Např. pro $n = 12$ patří $5^4 = 625 = 52.12 + 1$ do téže zbytkové třídy modulo 12 jako 1; $-3 \equiv 9 \pmod{12}$ protože $-3 - 9 = -12 = -1.12$.)

Zbytkovou třídu, do níž patří číslo a, vyznačujeme někdy pomocí pruhu nahoře, tedy jako $\overline{a}$, takže $\overline{a} = \overline{b}$ značí, že zbytková třída čísla a je táž, jako zbytková třída čísla b; chceme-li však přesněji vyznačit i modul n, dáme přednost způsobu psaní obvyklému v teorii čísel:

$$a \equiv b \pmod{n}$$

Je snadné nahlédnout, že všechna čísla celá se vlivem daného modulu n rozpadají do zbytkových tříd při čemž žádné číslo nepatří do dvou tříd současně a že tedy zbytkových tříd je právě tolik, kolik je nezáporných zbytků, které můžeme dostat při (částečném) dělení číslem n. Tyto třídy jsou tedy $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$.

Ze zbytkových tříd si nyní vybereme za prvky naší grupy jen zbytkové třídy těch zbytků, které jsou s modulem n nesoudělné (mají za největšího společného

dělitele číslo 1). Počet takových zbytků a tedy takových příslušných zbytkových tříd je $\varphi(n)$, pro $n = 12$ např. $\varphi(12) = 4$. Zde je třeba si uvědomit dvojí věc. Předně zbytek 0 není nesoudělný (= je soudělný) s číslem n, neboť $0 = n.0$ a $n = n.1$, tedy čísla 0 a n mají za největší společný násobek číslo n, čili třída $\overline{0}$, tj. třída všech násobků modulu n do naší grupy nepatří zatím co třída $\overline{1}$ samozřejmě do naší grupy patří. Za druhé, jestliže číslo a zanechává celý nezáporný zbytek r_a (při dělení modulem n) nesoudělný s n, pak i samo číslo a je s n nesoudělné. Takové číslo lze totiž vyjádřit (částečným dělením) jako

$$a = q.n + r_a$$

(kde číslo q je výsledek částečného dělení). Kdyby číslo a bylo dělitelno nějakým kladným dělitelem c modulu n, pak by tímto dělitelem c musel být dělitelný i rozdíl $a - q.n = r_n$ proti předpokladu. Ale právě tak i obráceně, jestliže číslo a je nesoudělné s modulem n, pak z právě naznačeného dělení čísla a modulem n, plyne nesoudělnost zbytku r_a s n, neboť jinak by i a bylo soudělné s n. Můžeme tedy prostě říci, že prvky naší grupy budou zbytkové třídy takových celých čísel, která jsou nesoudělná s modulem n a že naše grupa obnáší $\varphi(n)$ prvků.

Grupové násobení nyní zavedeme prostě takto: součinem $\overline{a}.\overline{b}$ dvou zbytkových tříd rozumíme tu zbytkovou třídu, do níž náleží (obyčejný) součin ab. Můžeme tedy definici našeho násobení tříd psát rovností

$$\overline{a}.\overline{b} = \overline{ab}$$

Např. pro modul $n = 12$ je $\overline{5}.\overline{7} = \overline{35} = \overline{11}$, protože $35 = 2.12 + 11$.

Jde již jen o to zjistit platnost grupových zákonů v naší, tzv. multiplikativní modulo n.

Axiom (1) neomezenosti a jednoznačnosti bude splněn, jestliže předně — kvůli jednoznačnosti — výsledek násobení $\overline{ab}$ třídy $\bar{a}$ třídou $\bar{b}$ bude týž, ať jej provedeme pomocí jakkoli zvolených čísel v té které zbytkové třídě. Věc tedy není nikterak samozřejmá, nýbrž máme ukázat, že jestliže a' patří do třídy $\bar{a}$ a b' do třídy $\bar{b}$, potom součin $a'b'$ patří do třídy $\overline{ab}$, čili že $\overline{a'b'} = \overline{ab}$. Skutečně, jestliže oba rozdíly $a' - a$ a $b' - b$ jsou dělitelny modulem n, pak i rozdíl

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b' - b) + \\ + b(a' - a)$$

je číslem dělitelným modulem n — jakožto součet dvou čísel jistě dělitelných číslem n.

Za druhé — kvůli neomezené proveditelnosti násobení musíme ukázat, že výsledek násobení dvou zbytkových tříd čísel nesoudělných s modulem n i součin těchto tříd (jak jsme si jej právě zavedli) je nejen vždy definován (což je již dostatečně zřejmo), ale že je to opět třída, do níž patří čísla nesoudělná s modulem. K tomu však stačí si uvědomit, že součin ab dvou čísel a a b obou nesoudělných s modulem n je opět číslo nesoudělné s n.

Axiom (2) asociativity je dán téměř bezprostředně pro naše násobení zbytkových tříd přenesením z asociativity násobení čísel samých. Neboť jsou-li a, b, c tři libovolná celá čísla, pak platí

$$\bar{a}.(\bar{b}.\bar{c}) = \bar{a}.\overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab}.\bar{c} = (\bar{a}.\bar{b}).\bar{c}$$

Axiom (3) jednotkového prvku je splněn pro zbytkovou třídu $\bar{1}$ (čísel, zanechávajících zbytek 1 při dělení modulem), jak ukáže následující úvaha: Nechť $i = q.n+$

$+ 1$ je číslo z třídy $\overline{1}$ (tj. $\overline{1} = \overline{i}$). Nechť dále libovolné celé číslo x je ze třídy $\bar{x} = \overline{r}$ kde r je nejmenší celý nezáporný zbytek při dělení čísla x modulem n. Pak lze psát $x = p.n + r$ (kde p je výsledek částečného dělení čísla x modulem n). Tedy

$$xi = ix = (pn + r)(qn + 1) = pqn^2 + n(p + rq) + r$$

takže součin $xi = ix$ dává při dělení modulem n týž zbytek r jako číslo x. Lze tedy psát opravdu pro zbytkové třídy žádanou rovnost

$$\bar{x}.\overline{1} = \overline{1}.\bar{x} = \bar{x}$$

Konečně axiom (4) inversního prvku si ověříme takto: Vypišme si jednotlivé nezáporné zbytky, nesoudělné s dělitelem n

$$a_1 = 1, a_2, a_3, \ldots, a_{\varphi(n)}$$

(Např. 1, 5, 7, 11 pro $n = 12$, $\varphi(n) = 4$.)

Když jsme zvolili libovolné číslo celé a, máme ukázat, že lze vždy nalézt celé číslo x tak, aby jeho zbytková třída $\bar{x}$ splňovala

$$\bar{x}.\bar{a} = \bar{a}.\bar{x} = \overline{1}$$

čili aby $ax \equiv 1 \pmod{n}$, to jest aby $\bar{x} = \bar{a}^{-1}$.

Vynásobme si proto po řadě naše nezáporné a s n nesoudělné zbytky s n nesoudělným číslem a, tj. utvořme čísla

$$aa_1 = a, aa_2, aa_3, \ldots . aa_n$$

(Např. tedy třebas pro $a = 7$, $n = 12$ čísla 7, 35, 49, 77.)

Ukažme, že *není možné*, aby mezi těmito součiny ani jeden *nedával* po dělení číslem n zbytek 1. Protože již víme, že všechna čísla a, aa_1, ..., $aa_{\varphi(n)}$ dávají vesměs zbytky nesoudělné s dělitelem n, znamenala by taková

možnost (kterou vyloučit je naším okamžitým cílem) to, že alespoň dvě čísla, řekněme aa_h a aa_k (pro $h \neq k$) z čísel $aa_1, aa_2, \ldots, aa_{\varphi(n)}$ by dávala tentýž nezáporný zbytek při dělení modulem n. Jinými slovy, rozdíl $aa_h - aa_k = a(a_h - a_k)$ by bylo číslo dělitelné modulem n. Protože a je číslo s číslem n nesoudělné, musel by být rozdíl $a_h - a_k$ dělitelný modulem n. To však právě není možné, protože a_k a a_h jsou čísla různá, nezáporná a menší než n.

Tedy aspoň jedno číslo aa_t (pro jedno z čísel $t = 1, 2, \ldots, n$) dá nezáporný zbytek 1 při dělení číslem n, takže pak lze položit $x = a_t$ a je $\bar{x}.\bar{a} = \bar{a}.\bar{x} = \overline{1}$. (V našem příkladě mezi čísly 7, 35, 49, 77 nalézáme $49 = 4.12 + 1 \equiv 1 \pmod{12}$, takže pro $\bar{a} = 7$ zrovna náhodou $\bar{a}^{-1} = \overline{7} = \bar{a}$.)

Tím je tedy dokončen důkaz, že zbytkové třídy čísel nesoudělných s dělitelem = modulem n tvoří při vytčeném násobení grupu řádu $\varphi(n)$, kde $\varphi(n)$ je počet s číslem n nesoudělných zbytků, jaké mohou vzniknout při částečném dělení číslem n.

Tím jsme však již také u našeho konečného cíle, tj. u malé Fermatovy věty. Jestliže totiž m je řád zbytkové třídy $\bar{a}$ (čísla a dle modulu n) jakožto prvku naší grupy, pak jednak platí

$$\bar{a}^m = \overline{1}$$

čili obšírněji

$$a^m \equiv 1 \pmod{n}$$

Za druhé však řád m prvku $\bar{a}$ naší grupy dělí řád $\varphi(n)$ této grupy, tedy $\varphi(n) = m.q$, kde q je celé kladné. Z toho ovšem plyne $\bar{a}^{\varphi(n)} = \bar{a}^{mq} = (\bar{a}^m)^q = \overline{1}^q = \overline{1}$ čili opravdu

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Poznamenejme ještě, že multiplikativní grupy tříd celých čísel nesoudělných s modulem n, jichž jsme právě užili ke grupově teoretickému důkazu malé Fermatovy věty, dávají bohatství příkladů konečných Abelových grup. V našem příkladě pro $n = 12$ to byla — až na isomorfii — nám známá Kleinova grupa čili grupa zákrytových pohybů obdélníka.

Rozumí se, že poslední úsudkový krok, který jsme učinili při důkazu malé Fermatovy věty lze učinit zcela stejně v libovolné konečné grupě. Tak dostáváme tzv. Fermatovu větu teorie grup, to jest tvrzení, že *v grupě řádu N je N-tá mocnina libovolného prvku rovna jednotce grupy*, tj. $a^N = j$, kde a je libovolně zvolený prvek, j je jednotka dané grupy.

Uveďme ještě dva důsledky rozdělení konečné grupy na (levé) třídy dle podgrupy. Předtím však je vhodné upozornit, že mezi podgrupy dané grupy počítáme logicky důsledně i ty dvě, které se vyskytují vždy, totiž grupu samu a podgrupu, skládající se jen z jediného prvku, jednotky dané grupy. Těmto podgrupám říkáme triviální podgrupy. (Kdybychom je z podgrup vyloučili, zkomplikovali bychom nevhodně znění příslušných pouček spoustou výjimek.)

Věta 6

Grupa, která má jen triviální podgrupy je konečná cyklická grupa řádu prvočíselného. Obráceně, konečné grupy prvočíselného řádu mají jen triviální podgrupy.

Důkaz je dán větou 5. Budiž totiž G nějaká grupa (konečná nebo nekonečná), o níž víme, že má jen triviální podgrupy. Zvolme v ní libovolný prvek různý od jednotky což lze učinit vždy kromě případu, že celá naše grupa G se skládá jen z jednotky. (V tom případě však

nemáme dále co dokazovat, jestliže považujeme i číslo 1 důsledně za prvočíslo, jakožto číslo nemající jiných kladných celých dělitelů kromě čísla 1 a sebe sama.)

Je-li tedy $a \neq j$ prvek z grupy, pak jsou dvě možnosti:

1. a je řádu konečného n a vytváří tedy cyklickou podgrupu řádu n, což je slučitelné s předpokladem jen tehdy, jestliže se tato cyklická podgrupa shoduje s celou grupou, takže G je v tomto případě konečná cyklická grupa řádu n. Kdyby n bylo číslo složené, $n = r.s$, kde r, s jsou nesoudělná čísla celá, kladná, různá od jednotky, pak by prvek $a^r \neq j$ vytvářel cyklickou podgrupu řádu s, skládající se z mocnin a^r, a^{2r}, a^{3r}, ..., $a^{sr} = j$, což předpoklad vylučuje. Tedy řád $n = p$ naší grupy G pouze s triviálními podgrupami, která se ukázala být cyklickou konečnou grupou, je prvočíslo p.

2. možnost: a vytváří v G nekonečnou cyklickou podgrupu

$$\ldots, a^{-2}, a^{-1}, j, a^1, a^2, \ldots$$

Potom však prvek a^2 vytváří v G netriviální cyklickou podgrupu, takže možnost 2 dle předpokladu odpadá.

Obrácené tvrzení, že grupy prvočíselného řádu nemají netriviální podgrupy, je bezprostředním důsledkem věty 5.

Věta 6 je jednoduchým příkladem na úplné určení typu isomorfie grupy předpokladem o řádu.

Věta 7

K tomu, aby část prvků konečné grupy tvořila podgrupu, stačí (a ovšem je i nutno), aby taková část obsahovala s každými dvěma prvky i jejich součin.

Důkaz: Předně dle předpokladu s prvkem a obsahuje předpokládaná část prvků grupy i mocninu a^N, kde

N je řád grupy; ta je však dle zmíněné tzv. Fermatovy věty teorie grup rovna jednotce.

Za druhé, je-li v naší části prvků grupy nějaký prvek x řádu n, pak dle předpokladu je tam i prvek $x^{n-1} = x^{-1}$. Více však k důkazu nepotřebujeme. — Je důležité si povšimnout nezbytnosti předpokladu konečnosti grupy: bez něho můžeme narazit na prvky nekonečného řádu a náš úsudek padá. V tom případě je nutno a stačí ještě dokázat přítomnost inversního prvku ke každému prvku v naší části, jež má být podgrupou, neboť přítomnost jednotky je již důsledkem.

Obraťme se k zásadně důležitému pojmu tzv. homomorfního zobrazení jedné grupy na druhou grupu.

Tento pojem je rozšířením nám již známého pojmu isomorfního zobrazení. Isomorfní zobrazení jedné grupy na druhou grupu věrně zachovává všechny grupové vlastnosti zobrazované grupy (originální), přenášejíc je dokonale na grupu obrazovou (na níž se zobrazuje originální grupa). V hrubém přirovnání je to tak, jako když znázorňujeme řekněme součást stroje školním modelem, který je sice z jiného materiálu (a popř. menších rozměrů), ale jehož tvar je přesně shodný s tvarem originálu.

Pro mnohé účely však stačí zmíněnou součást stroje kolmo *promítnout* na jednu průmětnu, to jest zobrazit útvar prostorový na útvar rovinný. Tím ovšem některé prostorové vlastnosti zanedbáme (nevystihneme), neboť různé body originálu se promítnou do jediného bodového obrazu v průmětně (celé hrany, kolmé k průmětně se zobrazí vždy jediným bodem). Zato však bývá průmět jednodušší a přehlednější než model a často dovoluje snadno nahlédnout (na výkrese) polohu promítané součásti ve stroji a její souvislost s ostatními částmi.

Abstraktní obdobu toho máme v teorii grup (a i v ostatních partiích abstraktní algebry): pojem vzájemně jednoznačného, isomorfního zobrazování jedné grupy na druhou rozšiřujeme v pojem homomorfního zobrazení jedné grupy na druhou. Zde tedy již i více prvků zobrazované originální grupy se může zobrazit na jeden jediný prvek grupy obrazové, při čemž se ovšem nadále součin dvou prvků zobrazované grupy zobrazí součinem příslušných obrazů. Homomorfní obraz grupy je tedy již obecně grupa, která podržuje jen některé grupové vlastnosti zobrazované grupy, neboť ostatní vlastnosti se při homomorfním zobrazování mohou porušit.

Uveďme si alespoň dva příklady homomorfního zobrazení (které nejsou isomorfními zobrazeními); je třeba si uvědomit, že isomorfní zobrazení se jeví zvláštním případem homomorfního zobrazení, kde *mohou*, ale *nemusí*, existovat dva a víc prvků majících týž obraz.

1. V prvém příkladě bude zobrazovanou grupou známá symetrická grupa S_n všech permutací stupně n (z n předmětů). Přitom si zavedeme několik pojmů, které budeme potřebovat i později.

Říkáme, že permutace π provedená na n čísel $1, 2, \ldots, n$ je **sudá** anebo **lichá** podle toho, zda v pořadí čísel $\pi(1), \pi(2), \ldots, \pi(n)$ došlo k sudému či lichému počtu porušení přirozeného sledu dvou čísel, čili k sudému, či lichému počtu **inversí**. Např. v permutaci $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ číslo 3 předešlo jednak 1 a jednak 2, 4 předešlo 2, máme tedy tři inverse a permutace π je lichá. Permutace $\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ je sudá, protože má celkem 8 inversí.

Přiřaďme libovolně zvolené permutaci π stupně n, jakožto prvku symetrické grupy S_n, číslo $+1$ anebo -1

podle toho, je-li tato permutace sudá či lichá. Takto přiřazené číslo k permutaci π označme jako $\varepsilon(\pi)$. Ukažme, že tím definované zobrazení je homomorfním zobrazením grupy S_n na (multiplikativní) grupu čísel $+1$ a -1, což je zřejmě cyklická grupa řádu 2. K tomu účelu vystihneme číslo $\varepsilon(\pi)$ (k dané permutaci π) takto: Znásobme si všechny rozdíly $\pi(h) - \pi(k)$, kde $h > k$. Pak součin (o zřejmém počtu $(n-1) + (n-2) + \ldots + 1 = \frac{(n-1).n}{2}$ činitelů) bude mít tolik záporných činitelů, kolikrát došlo k inversi při permutaci π, tedy to bude číslo kladné pro permutaci sudou a záporné pro permutaci lichou. Dělíme-li ještě tento součin jeho absolutní hodnotou, to jest součinem všech rozdílů $h - k$, kde $h, k = 1, 2, 3, \ldots, n$ a $h > k$, obdržíme právě číslo $\varepsilon(\pi)$. Krátce to lze vypsat formulkou

$$\varepsilon(\pi) = \prod_{h>k} \frac{\pi(h) - \pi(k)}{h - k},$$

kterou čteme: $\varepsilon(\pi)$ je součin přes všechna čísla

$$\frac{\pi(h) - \pi(k)}{h - k},$$

která lze utvořit, probíhají-li h i k všechna čísla od 1 do n, za podmínky, že h je větší než k.

Tato, zdánlivě neužitečně složitá formule (vzhledem k tomu, že $\varepsilon(\pi) = \pm 1$) dovoluje nejúsporněji dokázat, že $\varepsilon(\pi)$ dává skutečně homomorfní zobrazení grupy S_n na grupu $(+1, -1)$. Protože zřejmě existují jak permutace sudé, tak i liché každého stupně $n > 1$, takže jak čísla $+1$, tak i čísla -1 opravdu bude jako obrazů permutací vždy použito, jde jen o to dokázat, že součin permutací

se zobrazuje vždy součinem číselných obrazů jednotlivých násobených permutací, to jest, že platí

$$\varepsilon(\varrho\pi) = \varepsilon(\varrho).\varepsilon(\pi)$$

Skutečně, pišme číslo $\varepsilon(\varrho\pi) = \prod_{h>k} \frac{\varrho\pi(h) - \varrho\pi(k)}{h - k}$ po rozšíření jednotlivých zlomkových činitelů jako číslo

$$\prod_{h>k} \frac{\varrho\pi(h) - \varrho\pi(k)}{\pi(h) - \pi(k)} \cdot \frac{\pi(h) - \pi(k)}{h - k}$$

Znásobme si první zlomky zvlášť a druhé také zvlášť. Dostaneme tak

$$\varepsilon(\varrho\pi) = \prod_{h>k} \frac{\varrho(\pi(h)) - \varrho(\pi(k))}{\pi(h) - \pi(k)} \cdot \prod_{h>k} \frac{\pi(h) - \pi(k)}{h - k}$$

Zde druhý součin je již číslo $\varepsilon(\pi)$. První součin však není nic jiného, než číslo $\varepsilon(\varrho)$. Neboť probíhají-li h, k čísla 1, 2, ..., n, pak i $\pi(h)$ a $\pi(k)$ probíhají (obecně v jiném pořadí) tato čísla, takže i rozdíly $\pi(h) - \pi(k)$ proběhnou — až snad na znaménko — všechny kladné rozdíly různých dvou čísel, utvořené z čísel 1, 2, ..., n. Stane-li se však, že rozdíl $\pi(h) - \pi(k)$ je záporný (zatím co jsme předpokládali ve jmenovateli rozdíl kladný), pak to nevadí, neboť lze psát v takovém případě

$$\frac{\varrho(\pi(h)) - \varrho(\pi(k))}{\pi(h) - \pi(k)} = \frac{\varrho(\pi(k)) - \varrho(\pi(h))}{\pi(k) - \pi(h)}$$

kde $\pi(k) - \pi(h)$ je kladný rozdíl. Je tedy jedno, zda v prvním součinu násobíme přes všechny indexy h, k anebo přes odpovídající indexy $\pi(h)$, $\pi(k)$, takže první součin opravdu je vlastně $\varepsilon(\varrho)$. Máme tedy skutečně rov-

nost $\varepsilon(\varrho\pi) = \varepsilon(\varrho)\,\varepsilon(\pi)$ čili zobrazení ε je vskutku homomorfním zobrazením.

Je jasné, že zde homomorfní obraz, tj. cyklická grupa řádu 2, je hrubý a vystihuje symetrickou grupu permutací velmi málo.[21])

2. V druhém příkladě bude homomorfní obraz věrnější.

Budiž K (ze školy v podstatě známá) multiplikativní grupa komplexních čísel různých od nuly, vzhledem k násobení, danému rovností

$$(x_1 + i.y_1)\,(x_2 + i.y_2) = (x_1x_2 - y_1y_2) + \\ + i.(x_1y_2 + x_2y_1)$$

(kde i je známá komplexní imaginární jednotka).

Zobrazme grupu K do multiplikativní grupy R všech reálných čísel kladných tím, že přiřadíme komplexnímu číslu $x + iy$ jeho tzv. absolutní hodnotu $\sqrt{x^2 + y^2}$. Pak zobrazení

$$f(x + i.y) = \sqrt{x^2 + y^2}$$

je homomorfním zobrazením grupy K na grupu R.

Neboť opravdu, jednak každé komplexní číslo různé od nuly má jedinou kladnou absolutní hodnotu a každé reálné číslo je absolutní hodnotou komplexního čísla. A za druhé, absolutní hodnota součinu rovná se součinu absolutních hodnot jednotlivých komplexních činitelů, jak si čtenář ihned ověří na identitě

$$(x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 = (x_1^2 + y_1^2)\,(x_2^2 + y_2^2)$$

[21]) Říká jen, že sudá kráte sudá a lichá kráte lichá permutace je sudá, lichá krát sudá a sudá krát lichá permutace je lichá permutace.

Nyní je již na místě přesná abstraktní definice.

Definice

Buďtež G a H dvě grupy.

Říkáme, že grupa G je zobrazením f **homomorfně zobrazena na grupu** H, jestliže ke každému prvku x grupy G je zobrazením f přiřazen přesně jeden prvek $y = f(x)$ z grupy H tak, že jsou splněny tyto podmínky:

(i) Každý prvek y z grupy H splňuje vztah $y = f(x)$ alespoň pro jeden prvek x z grupy G. Slovy: Každý prvek grupy H je obrazem nějakého prvku, tzv. originálu neboli vzoru, z grupy G.

(ii) Pro libovolné prvky x_1 a x_2 z grupy G platí

$$f(x_1 x_2) = f(x_1).f(x_2)$$

(jestliže tečkou . odlišujeme grupové násobení v H od grupového násobení v G, jež zvláště nevyznačujeme). Slovy: Obraz součinu se rovná součinu obrazů.

Říkáme též, že grupa H je (jako celek) **homomorfním obrazem grupy** G (při zobrazení f). Možnost takového homomorfního zobrazení značíme symbolem

$$H \sim G$$

Uvědomíme si několik bezprostředních důsledků této definice. Každou grupu lze homomorfně zobrazit na grupu, skládající se jedině z jednotkového prvku; obrazem každého prvku je pak tento jediný (jednotkový) prvek. Takové zobrazení ovšem není příliš užitečné, protože naprosto deformuje zobrazovanou grupu.

Homomorfní zobrazení dává inversnímu prvku za obraz inversní prvek k obrazu, $f(x^{-1}) = f(x)^{-1}$, a jednotce j_G zobrazované grupy G přiřazuje jako obraz jednotku j_H grupy obrazů, $f(j_G) = j_H$.

Neboť $f(j_G) = f(j_G j_G) = f(j_G).f(j_G)$, z čehož druhý fakt plyne vynásobením prvkem $f(j_G)^{-1}$. První fakt pak již vyplývá z rovností

$$f(x^{-1}).f(x) = f(x^{-1}x) = f(j_G) = j_H$$

Nyní již není třeba zvláště podrobně vysvětlovat, co je to homomorfní reprezentace dané grupy grupou permutací anebo grupou matic. Je to přirozené a důležité rozšíření pojmu isomorfní reprezentace, s nímž jsme se již seznámili. Je zajímavé, že homomorfní reprezentace grupy (grupami permutací, nebo grupami matic) jakožto jakési „promítání" (při čemž za jednotlivé „průmětny" slouží symetrické grupy permutací stupně n, po případě grupy veškerých regulárních matic stupně n) prohlubuje zmíněnou obdobu s promítáním tělesa na dvě kolmé průmětny. I tu lze totiž úplně rekonstruovat původní grupu z jejich „průmětů", tj. homomorfních reprezentací (podobně jako si těleso zrekonstruujeme z jeho nárysu a půdorysu), jestliže známe tzv. úplný systém homomorfních reprezentací[22]) dané grupy, z něhož lze sestrojit isomorfní obraz dané grupy. Vedlo by nás příliš daleko, kdybychom měli na to podat příklady; čtenář, který se odhodlá k hlubšímu studiu teorie grup, je nalezne v obšírnějších učebnicích teorie grup.

Obrátíme se k dalšímu důležitému pojmu abstraktní teorie grup, který úzce souvisí s pojmem homomorfního zobrazení; je to již zmíněný pojem normální podgrupy, k němuž můžeme dospět takto:

Při každém homomorfním zobrazení f grupy G na grupu H nalézáme následující rozdělení prvků grupy G

[22]) Úplným nazýváme takový systém homomorfních reprezentací, v němž každý nikoli jednotkový originál obdrží alespoň jednou nikoli jednotkový obraz.

do tříd bez společných prvků: Každá taková třída sestává ze všech prvků x z grupy G, které mají týž obraz

$$y = f(x)$$

Tak v prvém předchozím příkladě se symetrická grupa S_n (všech permutací stupně n) rozpadá homomorfním zobrazením $f = \varepsilon$ (na cyklickou multiplikativní grupu z čísel ± 1) ve dvě třídy, třídu sudých a třídu lichých permutací. V druhém předchozím příkladě se multiplikativní grupa všech od nuly různých komplexních čísel, znázorněných body komplexní roviny (mimo počátek) rozpadá ve třídy čísel, znázorněných body na téže kružnici opsané okolo počátku.

Dále zjišťujeme, že třída všech originálů k jednotkovému prvku j_H — to jest třída všech x z G, pro něž $f(x) = j_H$ — tvoří podgrupu grupy G. — Neboť předně jestliže x_1 i x_2 jsou originály jednotky, $f(x_1) = j_H$, $f(x_2) = j_H$, potom i $f(x_1 x_2) = f(x_1).f(x_2) = j_H.j_H = j_H$, to jest pak i součin $x_1 x_2$ je originálem jednotky j_H v H. [To nám v případě konečné grupy již stačí (viz větu 7)]. Snadno se předvědčíme, že i ostatní podmínky, aby souhrn originálů jednotky (v homomorfním zobrazení) byl podgrupou, jsou splněny, takže naše tvrzení platí obecně. Neboť je nám již známo, že v homomorfním zobrazení je obrazem jednotky jednotka a obrazem inversního prvku je inversní prvek k obrazu původního prvku. Podgrupu (grupy G) originálů jednotky v našem homomorfním zobrazení grupy G na grupu H nazveme například N.

Vzniká přirozené podezření, zda ostatní třídy originálů se stejným obrazem (v homomorfním zobrazení) nejsou snad právě nám již známými levými třídami podle podgrupy N utvořenými v zobrazované grupě G. Toto podezření je oprávněné. Neboť jestliže x je daný

prvek v zobrazované grupě G a u je libovolný prvek z podgrupy N, potom součin xu má v grupě H za obraz prvek

$$f(xu) = f(x).f(u) = f(x).j_H = f(x)$$

tedy týž jako x. Stejně tak ovšem i obráceně, je-li xu (při u ležícím v podgrupě N) libovolný prvek levé třídy prvku x, pak jeho obraz $f(xu)$ je roven obrazu $f(x)$ libovolného prvku x z téže levé třídy v grupě G podle podgrupy N.

Utvoření tříd originálů se společným obrazem je tedy skutečně vlastně totéž co rozdělení prvků zobrazované grupy do levých tříd podle podgrupy, tvořené všemi originály jednotky. — Tím však celá věc zdaleka nekončí. Zjišťujeme totiž, že podgrupa N originálů jednotky se vyznačuje touto zvláštní vlastností: s každým prvkem x patří do N i každý prvek tvaru

$$zxz^{-1}$$

kde z je libovolný prvek ze zobrazované grupy G. Neboť jestliže je $f(x) = j_H$, pak následkem homomorfnosti zobrazení f je

$$f(zxz^{-1}) = f(z).f(x).f(z^{-1}) = f(z).j_H.(f(z))^{-1} = j_H$$

Podgrupám s touto důležitou vlastností (nezávisle na jakémkoli homomorfním zobrazení f) říkáme *normální podgrupy*.

Definice

Podgrupa N grupy G se nazývá normální podgrupou, jestliže s každým prvkem x patřícím do N patří do N i každý prvek zxz^{-1}, tzv. konjugovaný prvek k prvku x pomocí (libovolného) prvku z z grupy G.

Tak např. ze dvou nám známých podgrup grupy eu-

klidovských pohybů roviny (př. 2 ve 4. kap.) je podgrupa čistých posuvů normální podgrupou, kdežto podgrupa čistých otočení normální podgrupou není. — To vyplývá snadno z okolnosti, že provedeme-li otočení, pak posuv a nakonec zpětné otočení, dostáváme celkem opět čistý posuv (obecně ovšem jiný). Naproti tomu jestliže provedeme posuv, pak otočení a nakonec zpětný posuv, nedostáváme nikdy (pokud jde o neidentické pohyby) čisté otočení, nýbrž smíšený pohyb.

V příkladě s permutacemi všechny sudé permutace v symetrické grupě S_n tvoří tzv. alternující grupu A_n stupně n, která je normální podgrupou v grupě S_n. — V každé Abelově (komutativní) grupě je ovšem zřejmě každá podgrupa normální. (Obrácené tvrzení neplatí, viz cvič. 7 z 5. kap.)[23]).

Důležitost normálních podgrup v grupě vyplývá z toho, že pomocí nich lze z dané grupy tvořit potřebné nové grupy, jejímiž prvky se stávají celé (levé) třídy podle takové normální podgrupy. Násobení v takové grupě levých tříd dle normální podgrupy N grupy G je dáno takto: Jsou-li xN a yN dvě levé třídy (prvků x a y z G), potom za jejich součin $xN.yN$ položíme tu levou třídu, která obsahuje součin xy, to jest klademe

$$xN.yN = xyN$$

Dokažme, že axiomy grupy jsou pro toto násobení levých tříd splněny. K axiomu (1) máme vlastně jen zaručit, že výsledek násobení dvou tříd nezáleží na tom, jaké prvky si vybereme v jednotlivých třídách k vytvoření součinu tříd. To jest, máme ukázat, že jestliže

[23]) V grupě základních kvaternionů ze cvič. 7 z 5. kap. je každá podgrupa normální podgrupou, ačkoli grupa není Abelova.

$x' = xu_1$ a $y' = yu_2$, kde prvky u_1 a u_2 jsou z normální podgrupy N, potom součin $x'y' = xu_1yu_2$ patří do levé třídy součinu xy.

Skutečně lze psát $xu_1yu_2 = xyy^{-1}u_1yu_2$ a podle předpokladu normálnosti podgrupy N prvek $y^{-1}u_1yu_2$ patří do N, což právě potřebujeme.

Ostatní axiomy si ověříme ještě snadněji.

Axiom (2) nyní již lze dokázat prostým přenesením z celé grupy G do naší grupy levých tříd (dle N) rovnostmi

$$xyN.zN = (xy)\,zN = x(yz)\,N = xN.yzN$$

Axiom (3): úlohu jednotkového prvku v naší grupě tříd patrně bude hrát (následkem toho, jak jsme zaručili axiom (1) levá třída obsahující jednotku j_G grupy G, to jest sama normální podgrupa N.

Axiom (4): inversním prvkem k prvku (tj. ke třídě) xN je patrně třída $x^{-1}N$, protože součin $xN.x^{-1}N$ stejně jako $x^{-1}N.xN$ obsahuje jednotku j_G.

Grupě levých tříd v grupě G dle normální podgrupy N říkáme **faktorová grupa** grupy G dle normální podgrupy N a značíme ji G/N; normální podgrupě N se pak také někdy říká **normální dělitel**. Podle věty 5 je řád grupy G roven součinu řádu normální grupy N s řádem faktorové grupy G/N.

Jaký je zobrazovací vztah faktorové grupy G/N k původní grupě?

Odpověď je nasnadě: faktorová grupa G/N je homomorfním obrazem původní grupy G při zobrazení, přiřazujícím prostě prvku x z grupy G jeho levou třídu xN jakožto prvek z faktorové grupy G/N. Neboť to přímo říká definice $xN.yN = xyN$ násobení v G/N.

Vraťme se nyní k případu, že normální podgrupa N grupy G je souhrnem originálů jednotky v jakémsi homo-

morfním zobrazení f grupy G na grupu H. Jaký bude vztah faktorové grupy G/N ke grupě H?

Snadno nahlédneme, že tyto grupy jsou isomorfní. Zobrazení zprostředkující tento isomorfismus přiřazuje prostě třídě xN obraz $f(x)$, který má prvek x z grupy G v grupě H při výchozím homomorfním zobrazení f. Neboť takové zobrazení faktorové grupy G/N na grupu H je zřejmě homomorfní a kromě toho vzájemně jednoznačné. Shrňme si tedy výsledek předchozích úvah do následující tzv. první věty o isomorfismu teorie grup.

Věta 8

Jakmile podgrupa N grupy G je normální podgrupou, pak levé třídy xN (x je z G), do nichž se rozpadají prvky grupy G, tvoří tzv. faktorovou grupu G/N vzhledem k násobení $xN.yN = xyN$. Faktorová grupa G/N je homomorfním obrazem grupy G při homomorfním zobrazení $x \to xN$ přiřazujícím prvku x jeho levou třídu.

Je-li obráceně dána grupa H, která je homomorfním obrazem grupy G při zobrazení f, pak je tím určena normální podgrupa N všech originálů jednotky j_H grupy H tak, že faktorová grupa G/N je isomorfně zobrazena na grupu H zobrazením f, daným rovností

$$f(xN) = f(x)$$

Uvedená 1. věta o isomorfismu teorie grup (tento dlouhý titul je nutný, protože podobné věty o isomorfismu vystupují i v jiných částech abstraktní algebry) udává prostou, ale důležitou souvislost pojmu homomorfního zobrazení s pojmem normální podgrupy. Ve shora uvedených dvou příkladech se projevuje takto:

Faktorová grupa S_n/A_n symetrické grupy stupně n

podle její normální alternující podgrupy A_n je isomorfní s kteroukoli cyklickou grupou řádu 2, např. s podgrupou $(+1, -1)$ multiplikativní grupy všech zlomků.

Multiplikativní grupa kladných reálných čísel je isomorfní s faktorovou grupou všech komplexních čísel různých od nuly dle (normální) podgrupy všech komplexních čísel o absolutní hodnotě 1.

Uveďme ještě jeden důležitý příklad na tvoření faktorové grupy. Za grupu G vezměme aditivní grupu všech celých čísel; podgrupa N, která bude následkem komutativity samozřejmě normální, budiž tvořena všemi násobky pevně zvoleného celého kladného čísla n. Levé třídy dle N jsou nyní nám již známé zbytkové třídy dle modulu n, každá obsahuje všechna celá čísla, jež jsou navzájem kongruentní modulo n, tj. jež dávají při dělení modulem n týž nezáporný nejmenší zbytek.

Faktorová grupa G/N je tzv. **aditivní grupa modulo** n. (Pozor, něco jiného byla tzv. multiplikativní grupa modulo n, která se skládala jen ze zbytkových tříd, naplněných vesměs čísly, nesoudělnými s modulem, kdežto aditivní grupa modulo n obsahuje všechny zbytkové třídy.) Je-li H jakákoli cyklická grupa řádu n, např. multiplikativní grupa všech n-tých odmocnin z 1, pak první věta o isomorfii nám zde říká, že aditivní grupa modulo n je isomorfní s touto cyklickou grupou.

Tvořením faktorové grupy z grupy G podle normální podgrupy N ztotožňujeme vlastně prvky, patřící do téže levé třídy dle N v G. Zanedbávajíce rozdílnosti mezi prvky téže levé třídy, počínáme si obrazně řečeno asi tak, jako bychom se na naši grupu dívali (z jisté strany) z přiměřeně veliké dálky, až nám prvky z téže levé třídy splývají. Takový pohled dle první věty o isomorfismu je rovnocenný s daným „promítnutím" (tj. homomorfním zobrazením) dané grupy na jinou grupu H.

Normální podgrupy mají i jiné charakteristické vlastnosti, jimiž je možno je definovat. Hloubavý čtenář se rád přesvědčí, že:

a) Podgrupa U je normální tehdy a jen tehdy, když každá levá třída xU je rovna pravé třídě Ux téhož prvku x (všech pravých násobků ux prvků u podgrupy U násobených zprava prvkem x).

b) Podgrupa U je normální tehdy a jen tehdy, když souhrn $xUyU$ všech součinů násobků xu_1 s násobky yu_2 (kde u_1 a u_2 jsou libovolné prvky z podgrupy U a x a y jsou pevně zvolené prvky grupy) je vždy jistá levá třída podle U.

Na konec tohoto paragrafu si odvoďme důležitou tzv. druhou větu o isomorfismu teorie grup. Je to pomocná věta významu teoretického, jejíž užití si ukážeme v 6. kap.

Věta 9

Budiž G grupa, N její normální podgrupa a U její další podgrupa. Pak platí:

1. *Souhrn UN všech součinů un prvků u z podgrupy U s prvky n z normální podgrupy N je opět z podgrupa grupě G.* (Takový souhrn UN je tzv. spojení podgrup U a N.)

2. *Souhrn označený jako $U \cap N$ všech prvků grupy z G, které leží současně v podgrupě U i v normální podgrupě N, je rovněž podgrupou, a to dokonce podgrupou v grupě U.* (Takovému souhrnu $U \cap N$ říkáme průnik podgrup U a N.)

3. (*Vlastní tvrzení věty*):

Podgrupa N je normální podgrupou v grupě UN, podgrupa $U \cap N$ je normální podgrupou v grupě U a faktorové grupy UN/N a $U/(U \cap N)$ jsou navzájem isomorfní.

Důkaz: Nejprve k bodu 1:

Máme ukázat především, že součin dvou násobků tvaru u_1n_1 a u_2n_2, kde u_1, u_2 jsou libovolné prvky z podgrupy U a n_1, n_2 jsou libovolné prvky z normální podgrupy N (vše v G) je opět prvek tvaru un, kde u je z U a n je z N. Skutečně je

$$(u_1n_1)\,(u_2n_2) = u_1u_2(u_2^{-1}n_1(u_2^{-1})^{-1}n_2)$$

Protože N je normální podgrupa, leží v ní s prvky n_1 a n_2 též i prvek $n = u_2^{-1}n_1(u_2^{-1})^{-1}n_2$. Prvek $u = u_1u_2$ pak leží v U, protože U je podgrupa obsahující u_1 i u_2. Z rovností $(u_1n_1)^{-1} = n_1^{-1}u_1^{-1} = u_1^{-1}(u_1n_1^{-1}u_1u^{-1})$ je pak již snadno patrno, že UN je vskutku podgrupou v G.

Dále k bodu 2:

Je-li x i y jak v U tak i v N, pak platí totéž i o součinu xy, protože U, N jsou podgrupy. Jednotkový prvek j_G je ovšem jak v U, tak i v N. Je-li x v U i v N, pak ovšem totéž platí i o x^{-1}.

Konečně k hlavnímu bodu 3:

Předně je jasné, že N je podgrupou v grupě UN, neboť prvky n z N lze psát jako součiny jn kde j jednotka leží v U (jakožto v podgrupě). Je však samozřejmé, že N je normální podgrupou v grupě UN, neboť jestliže pro libovolný prvek z z G a kterýkoli prvek n z N je i konjugovaný prvek znz^{-1} v N, pak to tím spíše platí pro prvek z ležící v podgrupě UN.

Nyní již řádně definovaná faktorová grupa UN/N tvoří zřejmě podgrupu faktorové grupy G/N, protože obsahuje ty levé třídy dle N, které mají nějaký prvek v podgrupě U. Při nám známém homomorfním zobrazení $x \to xN$ celé grupy G na faktorovou grupu G/N zobrazíme tedy patrně podgrupu U (grupy G) tímto homomorfním zobrazením na faktorovou podgrupu UN/N. Nyní užijeme hlavní části 1. věty o isomorfismu.

V podgrupě U tvoří originály jednotky normální podgrupu N' tak, že faktorové grupy U/N a UN/N jsou navzájem isomorfní. Jednotkovým prvkem ve faktorové grupě UN/N je ovšem N (jakožto levá třída jednotky). Je zřejmo, že při homomorfním zobrazení $x \to xN$, omezeném na x z podgrupy U, budou mít N za obraz právě a jen ty prvky x z U, které současně leží v N, čili opravdu $N' = U \cap N$ je průnik U s N, což bylo dokázat.

Než přikročíme k další kapitole, zaveďme si ještě jeden základní pojem teorie grup: pojem jednoduché grupy.

Tak jako (vzhledem k dělitelnosti) hledíme celá (složená) čísla vystihovat čísly jednoduchými, tj. prvočísly, z nichž se (násobením) každé celé číslo dá složit, tak i při zkoumání grup a toho, jak se „skládají" ze svých podgrup a normálních podgrup nás zajímají nejprve podgrupy co možno „jednoduché". Slova „skládají" a „jednoduché" byla dána do uvozovek proto, že obdoba skládání celého čísla jako součinu prvočísel se „skládáním" grup z „jednoduchých" podgrup je neurčitá a mnohoznačná: Jak obratu „skládat grupu" tak výrazu z co možno „jednoduchých podgrup" možno dávat různé přesné významy, při nichž zmíněná obdoba s čísly je při mnohem větší složitosti grup jednou větší, jednou menší. O tom více v 7. kap.

Za jednoduchou budeme jistě považovat např. každou cyklickou grupu prvočíselného řádu, poněvadž ta, jak víme z věty 6 nemá žádné netriviální podgrupy, podobně jako prvočíslo nemá jiné dělitele (celé kladné) než triviální dělitele (sebe sama a jedničku). Kdybychom však omezili pojem jednoduché grupy na cyklické grupy prvočíselného řádu, byl by takový pojem pro většinu účelů příliš úzký.

Jako jednoduchou grupu definujeme raději grupu, která nemá žádné netriviální normální podgrupy. Takové grupy mají tedy, obrazně řečeno, tu vlastnost, že si je již nemůžeme zjednodušit a zmenšit tím, že je „pozorujeme z dálky" tvořením faktorové grupy. Jednoduché grupy jsou tedy jedním druhem základních stavebních kamenů obecných grup. Cyklické grupy prvočíselného řádu jsou zvláštním případem jednoduchých grup (které nemají vůbec netriviální podgrupy). Existují však také jednoduché nekonečné grupy (viz cvičení 7. za 7. kap. a při konečných grupách není jednoduchost grupy nikterak spojena s jednoduchostí jejího řádu (jak dále uvidíme).

Zvláštní a pro teorii rovnic důležitý druh konečných jednoduchých grup tvoří alternující grupy permutací stupně aspoň pátého. Těm se budeme věnovat v příští kapitole, čímž skončíme systematickou část výkladu základních pojmů teorie grup.

Mnohý z čtenářů bude snad ke své malé radosti konstatovat, že úvahy další kapitoly jsou obtížnější, než to, co předcházelo. Je to pochopitelné: prozatím jsme se omezovali na nejzákladnější pojmy teorie grup a jejich vzájemné nejjednodušší souvislosti. V podstatě jsme tím jen třídili bohatý materiál jevů, ovládaných grupovou zákonitostí, aniž jsme se o mnoho povznesli nad zevšeobecněňování poznatků známých v matematice i bez teorie grup. Úsudky byly sice mnohde dosti abstraktní, zato však velmi prosté a průhledné. Tam, kde teorie grup skýtá hlubší a podstatně nové výsledky, jež (jako např. v následujícím) vedly k novým matematickým objevům, tam je již třeba vyvinout značně větší myšlenkové úsilí, abychom dobře pochopili základní myšlenku důkazu a její realizaci. Pokusím se čtenáři toto pochopení co nejvíce usnadnit, tj. provést důkaz do

podrobností, při tom ale nenechat v těchto podrobnostech zaniknout hlavní motiv celé úvahy, jehož rozvíjením a ověřováním právě důkaz je.

Cvičení

1. Jaké jsou podgrupy v grupě S_3 (sledujte v tabulce zákrytových pohybů rovnostranného trojúhelníka; tabulka podgrupy je obsažena v tabulce grupy při vhodném přerovnání jako její čtvercová část při levém horním rohu).

2. Jaké jsou levé třídy dle podgrupy všech násobků čísla 3 (celých čísel tvaru $3k$, $k = \pm 1, \pm 2, \ldots$) v aditivní grupě celých čísel. Totéž pro násobky čísel 2, 4, 5. Jaké jsou vůbec všechny podgrupy aditivní grupy celých čísel?

3. Ukažte, že v symetrické grupě S_n (všech permutací z n čísel), všechny permutace, nechávající stát pevně různá daná čísla $k_1, k_2, \ldots k_r$, tvoří podgrupu, isomorfní s grupou S_{n-r}. Ukažte, že takové podgrupy jsou při stejném počtu r pevných čísel vzájemně isomorfní.
Jaké jsou levé třídy dle takové podgrupy pro $n = 3, 4$; $r = 1$; $k_1 = n$? (Udejte je výslovně.)

4. Proveďte tytéž úvahy, které v textu jsou provedeny pro levé třídy — i pro pravé třídy v grupě dle dané podgrupy.
Sledujte v grupě S_3 levé i pravé třídy dle téže podgrupy.

5. Ukažte, že každá podgrupa, dávající jen dvě levé třídy, je normální (v dané grupě).

6. Ukažte, že zobrazení $f(x) = |x|$ (absolutní hodnota z x) je homomorfní zobrazení multiplikativní grupy všech reálných čísel $\neq 0$ na multiplikativní grupu všech kladných čísel reálných.

7. Ukažte, že přiřadíme-li komplexnímu číslu $\alpha = x + iy$ jeho reálnou část $x = R(\alpha)$, pak R je homomorfní zobrazení aditivní grupy komplexních čísel α na aditivní grupu reálných čísel x. Totéž pro imaginární část $I(\alpha) = y$.

8. *Dokažte, že zobrazení

$$f\left\{\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}\right\} = a_1 b_2 - a_2 b_1$$

($a_{1,2}$, $b_{1,2}$ reálná anebo komplexní čísla) je homomorfní zobrazení grupy všech regulárních matic stupně 2 na multiplikativní grupu všech reálných (komplexních) čísel $\neq 0$. Jaká je tu odpovídající grupa originálů jednotky (čísla 1)? (Dle 1. věty o isomorfismu.)

9. Přesvědčte se, že matice tvaru

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

($a \neq 0$, tzv. diagonální matice) tvoří normální podgrupu v grupě všech regulárních matic stupně 2. Dokažte, že diagonální matice jsou komutativní s každou maticí stupně 2.

10. *Ukažte, se faktorová grupa dle normální podgrupy dle cvič. 9 je isomorfní s podgrupou všech matic $\begin{pmatrix} a_1 b_1 \\ a_2 b_2 \end{pmatrix}$ splňujících

$$a_1 b_2 - a_2 b_1 = 1$$

(Návod: Ve třídě, která je prvkem faktorové grupy, vyhledejte k libovolné tam ležící matici

$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

matici

$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \begin{pmatrix} \frac{1}{x_1 y_2 - x_2 y_1} & 0 \\ 0 & \frac{1}{x_1 y_2 - x_2 y_1} \end{pmatrix}$$

která v této třídě leží rovněž. Ukažte, že pro libovolnou matici téže třídy je tento součin táž matice a že tyto matice tvoří hledanou grupu tzv. grupu reprezentantů tříd, která je isomorfní s uvedenou faktorovou grupou.)

11. Co je dle 1. věty o isomorfii normální podgrupou originálů jednotky při homomorfním zobrazení $f(n) = i^n$ (i je imaginární jednotka) aditivní grupy celých čísel na multiplikativní grupu všech čtvrtých odmocnin z čísla $+1$?

12. Budiž G grupa, N její normální podgrupa, H její podgrupa. Jestliže podgrupy N a H nemají jiných společných prvků, než jednotku grupy, je faktorová grupa HN/N isomorfní s podgrupou H. Jestliže ještě každý prvek grupy G se dá psát jako součin prvku z H s prvkem z N, pak faktorová grupa G/N je isomorfní s podgrupou H. (Jako ve cvič. 10 je H pak grupou reprezentantů k faktorové grupě G/N.) Dokažte.

13. *Budiž G aditivní grupa všech celých čísel, U její podgrupa všech celých násobků čísla 4 a N její (normální) podgrupa všech násobků čísla 6. Pak grupa UN je podgrupa všech sudých čísel, průnik $U \cap N$ je podgrupa všech násobků čísla 12.

(Návod: 2 je největší společný dělitel čísel 4, 6; 12 je jejich nejmenší společný násobek.)

14. *Ukažte, že v př. 13 nám 2. věta o isomorfismu říká, že sečítání a odčítání sudých čísel modulo 6 je isomorfní se sečítáním a odčítáním všech celých čísel dělitelných čtyřmi, ale modulo 12.

7. kapitola

TŘÍDA KONJUGOVANÝCH PRVKŮ. NORMALISÁTOR PRVKU. TŘÍDOVÁ ROVNICE. KONJUGOVANÉ PERMUTACE. JEDNODUCHOST ALTERNUJÍCÍ GRUPY A_n PRO $n > 4$

Při pojmu normální grupy jsme narazili na pojem konjugovaných prvků v grupě (prvek y byl nazván konjugovaným s prvkem x pomocí prvku z, jestliže platilo

$$y = zxz^{-1})$$

Vzájemná konjugovanost prvků je jakási příbuznost, která dovoluje rozdělit důležitým způsobem prvky grupy do oddělených tříd vzájemně konjugovaných prvků (dle zcela jiného hlediska než rozdělení do levých tříd dle podgrupy).

Utvoříme-li totiž v grupě skupiny vzájemně konjugovaných prvků, pak zřejmě každý prvek grupy leží v (alespoň) jedné skupině a žádný neleží ve dvou či více skupinách současně. Neboť jakmile by prvek z byl konjugován jednak s prvkem x, jednak s prvkem y, čili jakmile by $z_1 x z_1^{-1} = z_2 y z_2^{-1}$, pak by

$$y = z_2^{-1} z_1 x z_1^{-1} z_2 = z_2^{-1} z_1 x (z_2^{-1} z_1)^{-1}$$

takže x by bylo konjugováno s y. Každá grupa G se tedy skutečně rozpadá ve třídy vzájemně konjugovaných prvků.

Některé třídy mohou ovšem obsahovat jen jediný

prvek. Především je jednotkový prvek j (v grupě G) konjugován sám se sebou, protože $xjx^{-1} = j$. V Abelových grupách je rozdělení do tříd konjugovaných prvků zřejmě nezajímavé, každá třída vzájemně konjugovaných prvků se tam skládá z jediného prvku.

Důležité je, že *počet vzájemně konjugovaných prvků je vždy dělitelem řádu grupy* (jestliže ovšem jde o grupu konečnou).

Abychom to ukázali, uvažme k danému prvku a konečné grupy G souhrn všech prvků x, které splňují vztah $a = xax^{-1}$, tj. $ax = xa$. (Říkáme, že x je prvek komutativní s prvkem a.) Mezi takové prvky patří předně jednotka j naší grupy G. Jestliže $a = x_1ax_1^{-1}$, $a = x_2ax_2^{-1}$, pak dosazením máme

$$a = x_1x_2ax_2^{-1}x_1^{-1} = x_1x_2a(x_1x_2)^{-1}$$

takže se dvěma prvky x_1 a x_2 i jejich součin x_1x_2 je komutativní s daným prvkem a. Konečně jestliže $a = xax^{-1}$, pak $x^{-1}ax = a$, čili spolu s x též inversní prvek x^{-1} je komutativní s a. Můžeme tedy říci, že *souhrn všech prvků komutativních s daným prvkem a z grupy G tvoří podgrupu N_a grupy G*, tzv. **normalizátor prvku a** v grupě G.

Všimněme si nyní levé třídy yN_a libovolného prvku y podle normalisátoru N_a prvku a. Ukazuje se, že všechny prvky yx z takové levé třídy skýtají týž k a konjugovaný prvek yay^{-1}. Neboť $yxa(yx)^{-1} = y(xax^{-1})\,y^{-1} = yay^{-1}$, podle definice normalisátoru N_a.

To tedy znamená, že různých konjugovaných prvků k prvku a je právě tolik, kolik je levých tříd v grupě G podle normalisátoru N_a, což je opravdu číslo, dělící (dle věty 3) řád grupy G.

Z toho tedy celkem vyplývá tento závěr:

Řád n konečné grupy G je součtem některých svých dělitelů, z nichž každý znamená počet vzájemně konjugovaných prvků v jedné třídě; mezi těmito děliteli, které se mohou i několikrát opakovat, vystupuje vždy číslo 1 jakožto počet všech prvků, konjugovaných s jednotkou grupy. To je slovní vyjádření tzv. třídové rovnice pro konečné grupy

$$n = 1 + h_2 + h_3 + \ldots + h_r$$

kde n je řád grupy, která se rozpadá do r tříd vzájemně konjugovaných prvků, při čemž i-tá třída obsahuje h_i prvků ($i = 1, 2, \ldots, r$) a první třída obsahuje jen jednotku grupy.

Všimněme si ještě jedné významné okolnosti, že totiž *řád každé normální podgrupy v dané grupě je součtem čísla 1 a některých ze sčítanců h_2 až h_r*, neboť normální podgrupa obsahuje ovšem jednotku grupy a s každým dalším svým prvkem obsahuje k němu i všechny prvky s ním konjugované. To je fakt, jehož se často využívá při hledání normálních podgrup dané konečné grupy.

Nyní se vraťme k permutacím, abychom viděli užití právě zavedených pojmů.

Budiž π nějaká permutace čísel $1, 2, \ldots, n$, převádějící číslo k v číslo $\pi(k)$. Pak libovolná s ní konjugovaná permutace $\varrho\pi\varrho^{-1}$ převádí číslo k v číslo $\varrho\pi\varrho^{-1}(k)$, tj. číslo $k = \varrho(i)$ v číslo $\varrho\pi\varrho^{-1}(\varrho(i)) = \varrho\pi(i)$. Čili provést permutaci $\varrho\pi\varrho^{-1}$ konjugovanou s permutací π pomocí permutace ϱ je totéž, jako současně v horní i dolní řádce rozepsané permutace π zaměnit tam stojící čísla podle permutace ϱ, tj.

$$\varrho\pi\varrho^{-1} = \begin{pmatrix} \varrho(1) & \varrho(2) & \ldots & \varrho(n) \\ \varrho\pi(1) & \varrho\pi(2) & \ldots & \varrho\pi(n) \end{pmatrix}$$

(Potřebujeme-li, přejdeme ovšem snadno k takovému vypsání, kde v první řádce jdou čísla podle velikosti.)

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

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

Avšak permutace, konjugované k dané permutaci a jejich počet lze ještě lépe přehlédnout pomocí tzv. rozkladu permutace v oddělené cyklické permutace, stručně v oddělené cykly. Cyklem $(i_1, i_2, \ldots, i_k)$ rozumíme při tom permutaci, která převádí číslo i_1 v číslo i_2, číslo i_2 v číslo i_3, atd. až číslo i_{k-1} v číslo i_k a číslo i_k zpět v číslo i_1, kdežto ostatní (nevyznačená) čísla nechává stát. Počet k čísel, která nepřejdou v sebe sama cyklickou permutací $(i_1, i_2, \ldots, i_k)$, nazýváme délkou cyklu. Cykly délky 2 (tvaru (ik)) se nazývají transposice; znamenají změnu čísla i v číslo k a čísla k v číslo i, při čemž ostatní čísla zůstávají stát. Dva cykly nazýváme oddělenými, jestliže není žádného čísla, které by se měnilo jak při jednom tak při druhém cyklu.

Dokážeme si tuto poučku:

Každá neidentická permutace stupně n (na n-číslech $1, 2, \ldots, n$) se dá jednoznačně rozložit v součin oddělených cyklů, při čemž na pořadí činitelů nezáleží.[24])

Budiž tedy π jakákoli neidentická permutace, provedená na číslech $1, 2, \ldots, n$. Najděme si první číslo i_1, které nezůstává stát při permutaci π, $\pi(i_1) \neq i_1$. Pak se mezi čísly $\pi(i_1), \pi^2(i_1), \pi^3(i_1), \ldots, \pi^t(i_1), \ldots$ musí některá opakovat, protože všech permutovaných čísel je jen konečně mnoho. Jestliže $\pi^r(i_1) = \pi^s(i_1)$ pro $r > s$; r, s celá kladná, pak $\pi^r(\pi^s)^{-1} = \pi^{r-s}(i_1) = i_1$.

[24]) Pochopitelně pro $n = 1$ máme pouze jedinou, a tedy identickou permutaci. — Pozn. red.

Existují tedy celá kladná čísla m taková, že $\pi^m(i_1) = i_1$. Budiž k nejmenší z takových čísel. Pak čísla $i_1, \pi(i_1), \pi^2(i_1), \ldots, \pi^{k-1}(i_1)$ jsou navzájem různá, avšak $\pi^k(i_1) = i_1$ (poprvé). Čísla i_1, $i_2 = \pi(i_1)$, $i_3 = \pi^2(i_1)$, $\ldots$, $i_k = \pi^{k-1}(i_1)$ skládají cyklus délky k, který působí patrně na ně právě tak, jako celá permutace π. Jestliže již není dalšího čísla, které se permutací π mění, jsme hotovi. V opačném případě proveďme s dalším číslem, které označme třebas m_1, totéž, co před tím s číslem i_1, takže obdržíme další cyklus, řekněme $(m_1 m_2 \ldots m_q)$, kde $m_2 = \pi(m_1)$, $m_3 = \pi^2(m_1)$, $\ldots$, $n_q = \pi^{q-1}(m_1)$, kdežto $\pi^q(m_1) = m_1$ (poprvé). Opět se daná permutace π a cyklus $(m_1 m_2 \ldots m_q)$ shodují co do svého účinku na čísla $m_1, \ldots . m_q$. Jedno a totéž číslo nemůže vystupovat v obou cyklech, protože jinak bychom měli $\pi^a(i_1) = \pi^b(m_1)$ při vhodných mocnitelích a, b, takže by číslo $m_1 = \pi^{a-b}(i_1)$ náleželo do prvního cyklu, proti předpokladu. Budeme-li tento postup opakovat tolikrát, kolikrát je možno, dosáhneme (následkem konečného počtu permutovaných čísel) nakonec toho, že všechna čísla, která danou permutací π nepřecházejí v sebe sama, se rozdělí do jednotlivých cyklů. Připomeňme znova, že každý takto získaný cykl je permutace, nechávající stát všechna čísla, kromě těch, která v cyklu vystupují — a čísla v cyklu vystupující zaměňuje stejně jako rozkládaná permutace. Konečně je zřejmo, že oddělenost cyklů, tj. okolnost, že žádné dva různé cykly nehýbají týmž číslem, má za následek jejich vzájemnou komutativitu. Tím je naše tvrzení dokázáno. Následující příklady na rozklad permutace v součin oddělených cyklů si dle potřeby čtenář pro větší jistotu sám doplní dalšími. (Pozor na to, že provedením cyklu —tj. cyklické permutace—na samotných číslech cyklu dostáváme týž cykl, jen jinak psaný!)

$$\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix} = (1\,3\,4\,2)\,[= (3\,4\,2\,1) = (4\,2\,1\,3) = (2\,1\,3\,4)]$$

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\10&4&5&9&1&8&7&2&6&3\end{pmatrix} =$$

$$= (1\ 10\ 3\ 5)\,(2\ 4\ 9\ 6\ 8)\,[= (4\ 9\ 6\ 8\ 2)\,(3\ 5\ 1\ 10) = \ldots]$$

(Je třeba pamatovat na to, že k určení permutace jejím rozkladem v cykly je třeba udat počet permutovaných předmětů (čísel), které jsou v cyklickém rozkladu vyznačeny.)

Podle předchozího nyní určíme permutaci $\varrho\pi\varrho^{-1}$, konjugovanou s permutací π pomocí permutace ϱ nejjednodušeji, je-li π dána rozkladem v oddělené cykly. Pak prostě nahradíme v takovém cyklickém rozkladu každé číslo i číslem $\varrho(i)$ a obdržíme tak konjugovanou permutaci $\varrho\pi\varrho^{-1}$ v rozkladu v oddělené cykly. Tak např., je-li π posléze uvedená permutace a ϱ je permutace

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\5&6&10&7&8&9&2&3&4&1\end{pmatrix}$$

pak v cyklickém rozkladu lze psát pohodlně

$$\varrho\pi\varrho^{-1} = (5\ 1\ 10\ 8)\,(6\ 7\ 4\ 9\ 3)$$

Samozřejmě tedy má konjugovaná permutace s danou permutací stejný počet cyklů téže délky. Ale patrně též obráceně, jestliže dvě permutace vykazují ve svých rozkladech v oddělené cykly týž počet cyklů stejné délky (pro každou se vyskytující délku cyklu), pak jsou tyto permutace vzájemně konjugované — a to pomocí každé permutace, která převádí vždy čísla jednoho cyklu v jedné permutaci v čísla cyklu téže délky v druhé permutaci.

Každou cyklickou permutaci možno dále ještě rozložit v transposice (dvojčlenné cykly), ovšem nikoli již oddělené, nýbrž naopak, navazující na sebe. Jestliže

$(i_1 i_2 \ldots i_k)$ je daný cyklus, pak patrně permutace jím dosažená je rovna sledu postupně provedených výměn (transposic) tak, že možno psát

$$(i_1 i_2 \ldots i_k) = (i_1 i_2)\,(i_2 i_3) \ldots (i_{k-2} i_{k-1})\,(i_{k-1} i_k)$$

[Pozor na to, že čteme a násobíme *od prava doleva*. Nejdříve si všimněme, že i_k přechází v i_{k-1} první transposicí, pak i_{k-1} přechází v i_{k-2} druhou transposicí atd., až posléze tento řetězec změn končí změnou i_2 v i_1, takže celý součin transposic převede i_k v i_1. Avšak pokud jde o i_{k-1}, již (zprava) první transposice převádí i_{k-1} v i_k a v žádné z následujících transposic se i_k už nevyskytuje, takže celkem náš součin transposic převádí i_{k-1} v i_k. Podobně dále i_{k-2} bude měněno až po připojení druhé (zprava) transposice, a to v i_{k-1}, kteréžto číslo již zůstane stát i po provedení dalších transposic. Stejně zjistíme i u ostatních čísel, že vypsaný součin transposic na ně účinkuje tak jako první transposice (zprava), v níž se toto číslo vyskytuje, tedy tak jako sám cykl.]

Z rozkladu cyklu v transposice vyplývá, že cykl o sudé délce je permutace lichá, jakožto součin lichého počtu transposic (což jsou permutace liché), a cykl o liché délce je permutace sudá, jakožto součin sudého počtu transposic (viz par. 5).

A nyní se obraťme k alternující grupě A_5 všech sudých permutací stupně 5.

Věta 10

Alternující grupa A_5 (sudých permutací z pěti předmětů) je jednoduchá.

Důkaz provedeme metodou, o níž již byla zmínka: určíme počet permutací ve třídách vzájemně konjugovaných permutací, na něž se rozpadá grupa A_5, a ukážeme prostě, že z čísla 1 a některých sčítanců, udávají-

cích počet konjugovaných permutací v A_5, nelze obdržet součet, který by dělil řád grupy A_5, tj. číslo, jež by mohlo být řádem normální podgrupy. Při tom musíme dát pozor na to, že půjde o konjugovanost v A_5 (a nikoli v S_5), tj. o konjugovanost pomocí sudých permutací.

Podle rozkladu v oddělené cykly nalézáme tyto druhy sudých permutací stupně 5 — jichž je $\frac{1}{2}5! = \text{řád } A_5 = 60$ (vedle identické permutace):

1. Součiny dvou (oddělených) cyklů, což musí být dvojčlenné cykly (transposice), aby permutace byla sudá
2. Jednotlivé trojčlenné cykly
3. Jednotlivé pětičlenné cykly

K 1. Všechny součiny dvou oddělených transposic, tedy permutace tvaru $(a_1a_2)\,(b_1b_2)$, (kde a_1, a_2, b_1, b_2 jsou různá čísla od 1 do 5), jsou konjugované se sudou permutací (1 2) (3 4) — a jsou tedy konjugované i navzájem. Neboť jedna z obou permutací

$$\begin{pmatrix}1&2&3&4&5\\a_1&a_2&b_1&b_2&c\end{pmatrix},\quad \begin{pmatrix}1&2&3&4&5\\a_2&a_1&b_1&b_2&c\end{pmatrix}$$

(c je jediné zbývající číslo různé od čísel a_1, a_2, b_1, b_2) je zaručeně sudá a pomocí obou obdržíme permutaci $(a_1\,a_2)\,(b_1\,b_2)$ jakožto konjugovanou k permutaci (1 2) (3 4) (dle svrchu uvedeného). Tvoří tedy součiny dvou oddělených transposic právě jednu třídu navzájem konjugovaných permutací v grupě A_5. Jejich počet obdržíme, kombinujíce každou z $\binom{5}{2}$[24]) dvojic čísel s $\binom{3}{2}$ zbý-

[24]) $\binom{n}{k}$ je ze školy známý binomický koeficient

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{1.2.3\ldots k}.$$

vajícími dvojicemi a dělíce dvěma, protože takto obdržíme každý součin dvou oddělených transposic dvakrát. Tedy první třída vzájemně konjugovaných permutací v grupě A_5 obsahuje $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ prvků.

K 2: Se třemi danými čísly a, b, c lze provést právě dva různé cykly, $(a\ b\ c)$ a $(b\ a\ c)$. Máme tedy $2 . \binom{5}{3} = 20$ trojčlenných cyklů v A_5. Ty jsou však všechny konjugované k cyklu (1 2 3), protože jedna z permutací

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

kterou žádané konjugovanosti lze dosáhnout, je jistě sudá. Druhá třída navzájem konjugovaných permutací v A_5 obsahuje tedy 20 prvků.

K 3: Pět čísel lze podrobit celkem $\frac{1}{5}5! = 24$ cyklickým permutacím, protože spolu s jedním pořadím pěti čísel i pět dalších pořadí, získaných z daného tou cyklickou záměnou, která je daným pořadím vyznačena, dává zápis téhož cyklu. (Na rozdíl od předchozího, nejsou všechny pětičlenné cykly vzájemně konjugovány v grupě A_5.) Je vidět, že jedinými permutacemi, pomocí nichž pětičlenný cykl je konjugován sám se sebou, je tento cykl sám a jeho mocniny. Jinými slovy, normalizátor pětičlenného cyklu v A_5 je tvořen právě všemi pěti různými mocninami tohoto cyklu. Ještě jinak řečeno, třída všech v grupě A_5 konjugovaných permutací k pětičlennému cyklu obsahuje

$$\frac{\text{řád } A_5}{5} = \frac{60}{5} = 12 \text{ permutací}$$

Rozpadá se tedy všech 24 pětičlenných cyklů v A_5 do dvou takových tříd vzájemně konjugovaných, obě po 12 permutacích (prvcích grupy A_5).
Třídová rovnice pro alternující grupu A_5 tedy zní

$$\tfrac{1}{5}5! = 60 = 1 + 15 + 20 + 12 + 12$$

Jako řády (netriviální) normální podgrupy v A_5 by tedy přicházela v úvahu jenom tato čísla (dle svrchu řečeného):

$$12 + 1 = 13,\ 15 + 1 = 16,\ 20 + 1 = 21$$
$$12 + 12 + 1 = 25,\ 15 + 12 + 1 = 28$$

Z nich však ani jedno neobstojí, nejsouc dělitelem řádu grupy, tj. čísla 60. — Tedy skutečně alternující grupa A_5 nemůže mít netriviálních normálních podgrup.
Ukazuje se, že všechny další alternující grupy jsou jednoduché. Myšlenku důkazu tohoto na první pohled překvapujícího jevu založíme, zhruba řečeno, v tomto: Na jedné straně netriviální normální podgrupa alternující grupy musí obsahovat dosti mnoho permutací, protože s každou permutací musí obsahovat značnou rozmanitost všech konjugovaných permutací. Na druhé straně však z předpokladu jednoduchosti alternující grupy A_n (která je ovšem podgrupou následující alternující grupy A_{n+1}) vyplývá (užitím 2. věty o isomorfismu), že naopak netriviální normální podgrupa v A_{n+1} musí obsahovat „velmi málo" permutací; z tohoto rozporu vyplývá, že nemá-li A_n netriviálních normálních podgrup, nemá je ani A_{n+1}. Protože však alternující grupa A_5, jak již víme, jednoduchá je, je jednoduchá i následující alternující grupa A_6, následkem toho je jednoduchá i další alternující grupa A_7, atd., až do nekonečna.
Náš postup důkazu jednoduchosti alternujících grup.

stupně vyššího než pátého, který následuje, je tedy tzv. *induktivním* postupem.

Věta 11

Alternující grupa A_n stupně n většího než čtyři je jednoduchá.

Důkaz: Alternující grupa A_5 je jednoduchá podle předchozí věty. Kdyby některá z dalších alternujících grup A_n pro $n > 5$ nebyla jednoduchá, musela by mezi nimi být jedna alternující grupa, řekněme A_m, co nejmenšího stupně m (ovšem že je $m > 5$) taková, že ona sama již jednoduchá není, ale předchozí alternující grupa A_{m-1} ještě jednoduchá je. Ukážeme, že existence takové první nikoli jednoduché alternující grupy A_m je vyloučena, protože by vedla k odporujícím si důsledkům.

Předpokládejme tedy, že máme v alternující grupě A_m ($m > 5$) netriviální normální podgrupu N (která tedy obsahuje více než jenom identickou permutaci).

Prvním naším (pomocným) krokem bude nalézt v N vhodnou permutaci ϱ a dvě z permutovaných čísel, řekněme i a k tak, aby čísla i, k, $\varrho(i)$, $\varrho(k)$ byla různá. — Zvolme proto v N libovolnou neidentickou permutaci σ, převádějící číslo i v číslo $\sigma(i) \neq i$ a rozložme σ v součin oddělených cyklů, jak byla o tom řeč shora. Jsou tři možnosti (vzhledem k tomu, že jde o sudé permutace):

a) máme více cyklických činitelů v rozkladu

b) rozklad se redukuje na jediný cykl, obsahující více než čtyři z permutovaných čísel

c) rozklad se redukuje na jediný, trojčlenný cykl

V obou případech a) a b) položme $\sigma = \varrho$; v případě a) pak vezmeme za i třebas libovolné číslo z prvního a za k libovolné číslo z druhého cyklu rozkladu, takže i, k, $\varrho(i)$, $\varrho(k)$ jsou zřejmě různá čísla. V případě b) vezmeme

třebas za i první a za k třetí číslo uvažovaného cyklu, takže $\varrho(i)$ bude druhé a $\varrho(k)$ čtvrté číslo tohoto cyklu, tedy opět jistě různá čísla.

V případě c) nechává permutace σ stát všechna čísla kromě tří. Můžeme pro jednoduchost předpokládat, že jde o čísla 1, 2, 3 a že $\sigma = (1\ 2\ 3)$ (toho lze vždy dosáhnout vhodným přečíslováním permutovaných předmětů). Konjugováním pomocí sudé permutace $(2\ 5)\ (1\ 4)$ (kterou dle předpokladu $m > 5$ máme k dispocici) zjišťujeme v naší normální podgrupě N přítomnost permutace

$$(2\ 5)\ (1\ 4)\ (1\ 2\ 3)\ (1\ 4)^{-1}\ (2\ 5)^{-1} = (4\ 5\ 3)$$

a tedy a přítomnost permutace

$$\varrho = (4\ 5\ 3)\ (1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & m \\ 2 & 4 & 1 & 5 & 3 & 6 & \dots & m \end{pmatrix} = (1\,2\,4\,5\,3)$$

Tím je případ c) převeden na případ b), který jsme již vyřídili.

Tedy opravdu máme vždy permutaci ϱ v N takovou, že čísla i, k, $\varrho(i)$, $\varrho(k)$ jsou různá.

Nyní provedeme druhý krok. Ten spočívá v důležitém zjištění, že z permutovaných čísel kterákoli dvě různá čísla r, s lze převést vhodnou permutací ϱ^*, obsaženou v N, v kterákoli dvě čísla r', s' (z permutovaných čísel) — pokud jen jsou čísla r, s, r', s' různá.

Za tím účelem si najdeme sudou permutaci π (v A_m), která převádí číslo i v číslo r, číslo k v číslo s, číslo $\varrho(i)$ v číslo r' a číslo $\varrho(k)$ v číslo s'[25]). Takovou sudou permutaci π si snadno sestrojíme prostě tak, že ještě určíme zcela libovolně v co mají přejít zbývající čísla — to jsou

[25]) Kdybychom nevěděli, že i, k, $\varrho(i)$, $\varrho(k)$ jsou různá čísla, nemohli bychom vždy s úspěchem permutaci π určit tak, jak to (níže) potřebujeme.

podle předpokladu ($m > 5$) alespoň ještě dvě — a není-li již takto daná hledaná permutace sudá, pak výměnou dvou naposled nahrazovaných čísel dosáhneme sudosti žádané permutace π.

Nyní však konjugovaná permutace $\varrho^* = \pi\varrho\pi^{-1}$, patřící spolu s ϱ do naší normální podgrupy N, převádí vskutku číslo r v číslo $\varrho^*(r) = \pi\varrho\pi^{-1}(r) = \pi\varrho\pi^{-1}\pi(i) = \pi(\varrho(i)) = r'$, a číslo s v číslo $\varrho^*(s) = \pi\varrho\pi^{-1}(s) = \pi\varrho\pi^{-1}\pi(k) = \pi(\varrho(k)) = s'$.

Tento krok nám již dovoluje udat číslo, jež musí být překročeno nebo alespoň dosaženo řádem naší normální podgrupy. Shledáváme totiž, že v N musí být $m - 3$ permutací, jimiž číslo 1 přechází v číslo 2 a při tom číslo m přejde v jedno z $m - 3$ zbývajících čísel. Stejně však musí N obsahovat dalších $m - 3$ permutací, převádějících číslo 1 v číslo 3 a současně číslo m ve zbývající čísla. Podobně vždy dalších $m - 3$ permutací v N je zaručeno při přechodu čísla 1 v čísla 4, 5, ..., m. Celkem tedy obsahuje naše normální podgrupa N nejméně $(m - 3)(m - 1)$ různých permutací; řád grupy N musí dosáhnout anebo překročit číslo

$$(m - 3)(m - 1) = m^2 - 4m + 3$$

A nyní se obraťme k obrácenému dohadu (se shora) řádu naší normální podgrupy.

K tomu užijeme 2. věty o isomorfismu. Pokládáme za podgrupu U (z věty 9) předchozí alternující grupu A_{m-1} všech těch sudých permutací na m předmětech (číslech), které nechávají jistý předmět (číslo) stát; za normální podgrupu N ve větě 9 vezmeme ovšem N a za celou grupu G samozřejmě celou alternující grupu A_m. Pak máme isomorfismus

$$A_{m-1}/(A_{m-1} \cap N) \cong (A_{m-1}N)/N$$

kde si zatím ještě ponecháváme možnost stanovit předmět (číslo), jejž mají nechat stát permutace z A_{m-1}. Průnik $A_{m-1} \cap N$ značí normální podgrupu v grupě A_{m-1} všech permutací, jež patří jak do A_{m-1}, tak i do naší normální podgrupy N.

Předmět, tj. číslo, které mají nechat stát permutace z A_{m-1}, si nyní zvolíme tak, aby podgrupa N, (která byla předpokládána jako netriviální, tj. různá od celé grupy A_m), neobsahovala podgrupu A_{m-1}, čili aby průnik $A_{m-1} \cap N$ nebyl roven A_{m-1}. Že to vždy lze (za našich předpokladů), to poznáme takto: V opačném případě by N musela obsahovat každou z možných podgrup A_{m-1} (pro různě zvolená, při permutacích stálá čísla), tj. N by obsahovala veškeré sudé permutace (na našich m předmětech, resp. číslech), které nechávají stát aspoň jedno číslo. Jakožto podgrupa obsahovala by N veškeré součiny takových permutací. Avšak tím by již N obsahovala všechny sudé permutace (stupně m) vůbec. Neboť rozložme každou z dalších sudých permutací (tj. takových, které nenechávají stát nic) v součin oddělených cyklů. Dále rozložme tyto cykly v součiny transposic (tak jak jsme to uvedli shora) a konečně sdružme tyto (více než tři) posléze získané činitele (transposice) do dvou činitelů vždy o sudém počtu transposic. Tak se stává opravdu sudá permutace součinem dvou sudých permutací, z nichž každá nechává aspoň jedno permutované číslo stát.

Zvolivše si tedy podgrupu A_{m-1} v A_m tak, aby nebyla obsažena v normální podgrupě N, máme v průniku $A_{m-1} \cap N$ normální podgrupu (pod)grupy A_{m-1}, která je od A_{m-1} různá. Avšak A_{m-1} je podle předpokladu ještě jednoduchá grupa, tedy nezbývá než že $A_{m-1} \cap N$ se redukuje na pouhou jednotku (identickou permutaci).

Následkem toho však faktorová grupa $A_{m-1}/(A_{m-1} \cap N)$ je prostě grupa A_{m-1} sama. Nahoře naznačený isomorfismus nám tedy mimo jiné praví to, že faktorová grupa $(A_{m-1}N)/N$ má týž řád, jako má A_{m-1}, což je číslo $\frac{(m-1)!}{2}$; toto číslo je tedy rovno řádu grupy $A_{m-1}N$ dělenému řádem normální podgrupy N (viz věta 5). Avšak řád grupy $A_{m-1}N$ jakožto podgrupy v A_m je nanejvýše roven číslu $\frac{m!}{2}$ (což je řád A_m). Máme tedy

$$\frac{(m-1)!}{2} \leqq \frac{m!}{2} \frac{1}{\text{řád } N}$$

z čehož plyne, že řád naší normální podgrupy N grupy A_m je nanejvýše roven číslu m.

Avšak prve jsme dokázali, že řád grupy N musí být větší anebo nejvýše roven číslu $m^2 - 4m + 3$. Z toho ovšem vyplývá, že $m^2 - 4m + 3 \leqq m$, tj. že číslo

$$m - (m^2 - 4m + 3) = 5m - (m^2 + 3)$$

je nezáporné, čili i číslo

$$(5m - [m^2 + 3]) : m = 5 - \left(m + \frac{3}{m}\right)$$

je nezáporné. Ale to právě není pro předpokládané $m > 5$ možné. Dospěli jsme tedy k hledanému logickému rozporu, plynoucímu z předpokladu, že existuje alternující grupa A_m pro $m > 5$, která by nebyla jednoduchá; tím je tedy takový předpoklad vyvrácen a věta o jednoduchosti alternujících grup permutací stupně alespoň pátého dokázána.

Seznání jednoduchosti alternujících grup A_n všech stupňů n, vyšších, než 4 bylo důležitým krokem v počátcích samotné teorie grup, protože se ukázalo, jak složitými (vzhledem k rozmanitosti podgrup těchto alternujících grup) mohou být jednoduché grupy (jednoduché vzhledem k tomu, že nemají normální netriviální podgrupy). Jak jsme však již naznačili, má tento poznatek značný význam i mimo teorii grup, v tzv. Galoisově[26]) teorii algebraických rovnic tvaru

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

tj. tzv. algebraických rovnic stupně n o jedné neznámé x. V této souvislosti byla také jednoduchost alternujících grup objevena. Není možno podat zde ani přibližný výklad Galoisovy teorie. Musíme se spokojit s pouhým poukazem na to, že Galoisova teorie převádí vlastnosti algebraické rovnice o jedné neznámé ve vlastnosti jisté tzv. Galoisovy grupy permutací kořenů této rovnice. Vlastnostem grupy odpovídají vlastnosti rovnice a naopak. Zejména řešitelnosti rovnice pomocí tzv. algebraických početních úkonů (sečítání, odčítání, násobení, dělení, mocnění, odmocňování) odpovídá jistá vlastnost (příslušné Galoisovy) grupy; tato vlastnost byla proto nazvána řešitelnost grupy. Z jednoduchosti alternujících grup stupňů vyššího než čtyři vyplývá, že Galoisova grupa obecné rovnice stupně vyššího než čtyři *není řešitelná*. Tedy neexistují byť sebe složitější vzorce, které by dovolovaly vypočítat (pomocí šesti algebraických úkonů) hodnoty jednotlivých kořenů rovnice pátého, šestého a vyššího stupně podobně, jako

[26]) Pěkný výklad Galoisovy teorie nalezne čtenář např. v polské učebnici vyšší algebry: Sierpiński, *Zarys algebry wyszej* (Monografie matematyczne Warszawa 1948) jako dodatek od prof. Mostowského.

je tomu u rovnic druhého (to čtenář zná), třetího a čtvrtého stupně (to čtenář možná nezná, ale takové vzorce pro rovnice druhého, třetího a čtvrtého stupně byly známy již počátkem novověku, viz Schwarzovu knížku „O rovnicích"). Objev neřešitelnosti rovnic stupně vyššího než čtyři algebraickým vzorcem, a co více, nalezení konkrétních příkladů rovnic s celočíselnými koeficienty, jichž žádný kořen se nedá vytvořit pomocí vyjmenovaných šesti algebraických početních úkonů, prováděných s koeficienty rovnice, patří k největším objevům algebry na počátku 19. století, na nichž se podílejí nejméně tři matematikové: Ital Ruffini, Francouz Galois a Nor Abel. Tímto objevem definitivně skončilo marné hledání vzorců pro řešení rovnic pátého a vyššího stupně, které trvalo dobrá tři staletí.

Po tomto, bez tréninku a napoprvé jistě namáhavém výstupu, který jsme krok za krokem provedli, věnujeme se nyní již jen klidnému rozhledu z relativního vrcholku, jehož jsme právě dosáhli, tj. pohledu na některé další a vyšší vrcholky teorie grup. Řečeno méně obrazně (a pro čtenáře, jenž nemá v oblibě turistiku) v další a závěrečné kapitole našeho výkladu základních pojmů teorie grup půjde již jen o informativní přehled některých hlavních výsledků a užití teorie grup, které podáme bez důkazů.

Cvičení

1. Proveďte vynásobení cyklů

a) $(1\ 4\ 2)\,(5\ 3\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \varrho$

b) $(3\ 5)\,(1\ 2\ 8\ 7)\,(6\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \sigma$

c) Pro cykl $\pi = (1\ 2\ 3\ 4\ 5\ 6)$ udejte všechny vzájemně různé mocniny $\pi^2, \pi^3, \ldots$ (Přesvědčte se, že mocnina cyklu obecně není již jediný cykl: $\pi^2 = (1\ 3\ 5)\ (2\ 4\ 6)$; ale ovšem $(1\ 3\ 5)^3 = (1\ 5\ 3)$. *Jaké pravidlo mocnění cyklů lze vyslovit pro to, kdy se cykl mocněním rozpadá?

2. Najděte konjugované permutace

$$\varrho\pi^3\varrho^{-1},\ \sigma\varrho\sigma^{-1},\ \varrho\sigma\varrho^{-1},\ \pi^3\varrho\pi^{-3}$$

k permutacím π^3, ϱ, σ ze cvič. 1.

3. Proveďte rozdělení permutací do tříd konjugovaných pro grupy S_3 a S_4 podrobně. Napište třídové rovnice.

4. Řád permutace je nejmenším společným násobkem délek oddělených cyklů v rozkladu. — Dokažte!

5. Nazveme sudou permutaci π' všech přirozených čísel 1, 2, ... každou sudou permutaci π nějakých n čísel, která byla doplněna předpisem $\pi'(n+1) = n+1$, $\pi'(n+2) = n+2$, ... atd. bez omezení. (Zatímco $\pi'(k) = \pi(k)$ pro $k = 1, 2, \ldots, n$). Je tedy π' předpis, přiřazující každému přirozenému číslu přesně jedno přirozené číslo, při čemž jen konečně mnoho čísel obdrží tímto přiřazením číslo od daného čísla různé; (sudá permutace všech přirozených čísel nechává stát skoro všechna čísla, až na konečný počet výjimek; tato výjimečná čísla jsou podrobena jisté sudé permutaci v obvyklém smyslu).

Dokažte, že sudé permutace přirozených čísel tvoří (nekonečnou nekomutativní) grupu A při definici násobení

$$[\pi'.\varrho']\ (r) = \pi'(\varrho'(r)) \text{ pro } r = 1, 2, \ldots$$

Dokažte, že grupa A obsahuje podgrupy A_n pro $n = 1, 2, 3, \ldots$ vesměs isomorfní s grupami A_n všech sudých permutací prvních n čísel $1, 2, \ldots, n$; dále dokažte, že každý prvek z grupy A (sudá permutace přirozených čísel) je obsažen v některé z podgrup A_n.

6. *Dokažte, že nekonečná grupa A neobsahuje vlastní normální podgrupu čili že je příkladem nekonečné jednoduché grupy.

(Návod: Kdyby N byla normální podgrupa v A, pak průnik $A'_n \cap A$ by byla normální podgrupa v podgrupě A'_n (jak víme z 2. věty o isomorfii). Následkem jednoduchosti podgrup

A'_n pro $n = 5, 6, 7, \ldots$ (dle cvič. 6) musí buďto: $A'_n \cap N = A'_n$ čili A'_n je podgrupou v normální podgrupě N anebo: $A'_n \cap N$ obsahuje jen identickou permutaci (jednotku). Nastává-li druhá možnost pro všechna $n = 5, 6, 7$ pak snadno ukážete, že N obsahuje jen jednotku. V opačném případě $A'_m \cap N = A'_m$ pro jisté $m > 5$ zase snadno ukážete, že N obsahuje každou podgrupu A'_r pro $r > m$, a tedy že N je rovna celé grupě A.)

7. Dokažte jednoduchost všech alternujících grup A_n pro $n \neq 4$.

8. kapitola

KOMPOSIČNÍ ŘADY. DIREKTNÍ ROZKLADY. p-GRUPY A SYLOWOVY PODGRUPY. GRUPY A TOPOLOGIE

Jedním z hlavních úkolů teorie grup, jak již bylo poznamenáno, je probádat, jak jsou grupy budovány ze svých podgrup. Jsou dva hlavní způsoby, kterými sledujeme jak podgrupy skládají grupu: tzv. komposiční řada a tzv. direktní rozklad grupy.

Oč běží při komposiční řadě?

Chceme-li alespoň hrubě přirovnat tvoření (klesající) komposiční řady podgrup k něčemu názornému, napadá nás obdoba s postupným vysunováním částí z částí při rozkládání nohy trubkového skládacího fotografického stativu: Nejprve se vysune z celku v něm obsažená co nejobjemnější část, z této části opět v ní obsažená co největší část — a to se opakuje tolikrát, až naposledy vysunutá trubková část v sobě již nemá další vysunovatelnou část, a až je jisto, že žádné dvě trubky již nejsou do sebe zasunuty.

V grupě se postupně vysunovanými částmi ovšem rozumějí podgrupy. Opravdu přehledná zákonitost se však při tom objevuje jen tehdy, když předpokládáme ještě, že „vysunovaná" podgrupa je vždy normální podgrupou (nikoli nutně v celé grupě, ale) v té podgrupě, z níž je právě vysunována.

Přistupme od podobenství k definici.

Mějme v grupě G jistý počet n podgrup $G_1, G_2, G_3, \ldots, G_n$ tak, že jsou splněny tyto podmínky:

1. G_1 je celá grupa G, G_n je podgrupa (j), která se skládá jen z jednotky j grupy G.

2. G_{i+1} je netriviální normální podgrupa v G_i $(i = 1, 2, \ldots, n - 1)$.

3. Neexistuje již žádná podgrupa G' v G, která by se dala vložit mezi některé dvě podgrupy G_i a G_{i+1} tak, aby G' byla netriviální normální podgrupou v G_i a sama aby obsahovala G_{i+1} jako netriviální normální podgrupu.

Potom říkáme, že podgrupy $G_1, G_2, G_3, \ldots, G_n$ tvoří tzv. **komposiční řadu grupy** G. Počtu n podgrup v komposiční řadě vystupujících se říká **délka** komposiční řady. Faktorovým grupám G_i/G_{i+1} říkáme někdy **faktory** komposiční řady. Je důležité si povšimnout, že podmínku 3 lze právě tak dobře nahradit podmínkou 3′:

3′. Faktory komposiční řady, tj. faktorové grupy G_i/G_{i+1} jsou jednoduché grupy. (Neboť každá normální podgrupa G' grupy G_i, obsahující grupu G_{i+1} dává vznik normální podgrupě G'/G_{i+1} faktorové grupy G_i/G_{i+1} a obráceně.)

Uveďme si alespoň dva příklady komposiční řady:

1. Symetrická grupa S_n pro $n \geqq 5$ má komposiční řadu S_n, A_n, (i) (i nechť je identická permutace, (i) grupa skládající se jen z i) délky 3, a dá se dokonce snadno ukázat, že jiných komposičních řad nemá. Alternující podgrupa A_n v S_n je tam totiž normální podgrupou, neboť se sudou permutací ϱ je i každá s touto konjugovaná permutace $\pi\varrho\pi^{-1}$ sudá — a faktorová grupa S_n/A_n je, jak víme, cyklická grupa řádu 2, tedy grupa jednoduchá; alternující grupa A_n je pak sama již, jak víme z předchozího paragrafu, jednoduchá grupa.

2. Cyklická grupa řádu 12, skládající se z mocnin

$$a, a^2, a^3, \ldots, a^{12} = j$$

má kompoziční řadu složenu ze 4 následujících cyklických podgrup; celá grupa (a) sama (tvořena všemi mocninami prvku a), podgrupa (a^3) vytvořená 4-mi různými mocninami a^3, a^6, a^3, $a^{12} = j$ prvku a^3, podgrupa (a^6) této podgrupy, tvořená dvěma různými mocninami a^6, $a^{12} = j$ prvku a^6 a konečně jednotková podgrupa (j).

Avšak to není jediná kompoziční řada. Jiná kompoziční řada se skládá z podgrup (a), (a^2) (a^6), (j) — při stejném vyznačování cyklických grup. (O normálnost podgrupy v předchozí podgrupě kompoziční řady se zde netřeba starat — vzhledem ke komutativitě dané grupy.)

O kompozičních řadách platí nyní pozoruhodná věta Jordan-Hölderova, která dalekosáhle odhaluje strukturní uložení podgrup v grupě:

Délka dvou různých kompozičních řad téže grupy je táž. Co více, ke každému faktoru jedné kompoziční řady existuje s ním isomorfní faktor druhé kompoziční řady, takže faktory obou kompozičních řad jsou až na isomorfismus a pořadí tytéž.[27])

[Povšimneme si, že Jordan-Hölderova věta sama nás nepoučuje o tom, zda daná grupa vůbec kompoziční řadu má, ona jen vypovídá o vlastnostech kompozičních řad v případě, že nějaké máme. Existence kompozičních řad je zřejma v případě konečných grup. V zobecnění na

[27]) Francouz C. Jordan objevil rovnost délek kompozičních řad téže grupy. Němec O. Hölder později objevil tvrzení o „rovnosti" (tj. isomorfismu) faktorů. Dalekosáhlé zobecnění na kompoziční řady „nekonečné" délky podal sovětský matematik A. Kuroš. Dalším vyšetřováním platnosti zobecněné Jordan-Hölderovy věty ve svazech se zabýval u nás V. Kořínek.

nekonečné grupy je podstatné, zda jdeme od větších podgrup k menším (klesající komposiční řada) anebo naopak, od menších podgrup k větším (stoupající komposiční řada). Pro klesající komposiční řady i „nekonečné" (nemůžeme zde tento pojem blíže vysvětlovat, neboť bychom k tomu potřebovali pojem nekonečného ordinálního čísla, viz např. Pospíšilovo „Nekonečno v matematice" ve sbírce „Cesta k vědění") věta Jordan-Höldera platí, pro stoupající nikoli. Jordan-Hölderova věta má rovněž značný význam ve zmíněné již Galoisově teorii algebraických rovnic; v souvislosti s ní byla tato věta objevena koncem minulého století.]

Od postupného rozkladu vysouváním podgrup rozkládané grupy se obraťme k jinému druhu rozkladu, který spíše připomíná rozklad přirozeného čísla v součin mocnin prvočísel: je to tzv. direktní rozklad grupy.

Ze školy je, resp. má nám být dobře známo, že každé přirozené číslo se dá psát jednoznačně (až na pořadí činitelů) jako součin mocnin různých přirozených prvočísel $p_1, p_2, \ldots, p_r$, tedy

$$a = p_1^k p_2^{k_1} \ldots p_r^{k_r}$$

Rozkládáme-li takto přirozené čitatele i jmenovatele kladných zlomků a připouštíme-li za mocnitele prvočísel i čísla záporná, pak napsaný rozklad v mocniny prvočísel platí i pro každé kladné číslo lomené a, tedy pro každý prvek multiplikativní grupy kladných racionálních čísel. Při tom všechny mocniny jednoho a téhož prvočísla p s kladnými i zápornými mocniteli

$$\ldots, p^{-2}, p^{-1}, p^0 = 1, p^1, p^2, \ldots$$

tvoří zřejmě normální (nekonečnou cyklickou) podgrupu v multiplikativní grupě kladných racionálních čísel.

Každé kladné racionální číslo je tedy až na pořadí činitelů jednoznačně daným součinem činitelů vzatých z jednotlivých takových normálních podgrup, dvě takové normální různé podgrupy nemají více společných prvků (racionálních čísel), než jen jednotku, a čísla (prvky), patřící do jedné takové normální podgrupy (tvořené všemi mocninami určitého prvočísla) se již takto dále rozkládat na nesoudělné činitele nedají.

Od takovéhoto pohledu na rozklad lomených čísel v součin mocnin prvočísel dojdeme snadno k příslušnému zobecnění na grupy vůbec, tj. k pojmu direktního rozkladu grupy v direktně nerozložitelné podgrupy:

Budiž G nějaká grupa. Může se stát, že existují netriviální normální podgrupy $G_1, G_2, \ldots$, grupy G tak, že každý prvek g z grupy G se dá až na pořadí činitelů *jediným způsobem* psát jako součin konečného počtu činitelů $g = g_1 . g_2 \ldots g_n$, kde činitel g_i $i = 1, 2, \ldots$) patří do normální podgrupy G_i.

Říkáme, že tím je dán direktní rozklad grupy G a píšeme

$$G = G_1 \times G_2 \times \ldots$$

Normální podgrupy G_i se pak jmenují direktní faktory (direktního) rozkladu. Jestliže se tyto direktní faktory G_i samy již nedají stejným direktním způsobem rozložit, říkáme, že jsou to (direktně) nerozložitelné (ireducibilní) grupy. (Pozor, nerozložitelnost je tedy něco jiného — pro grupy — než jednoduchost; jednoduchá grupa je jistě nerozložitelná, ne vždy však obráceně, jak je vidět na nekonečné cyklické grupě: ta je direktně nerozložitelná, není však jednoduchá.)

Máme tu tedy dvojí obdobu s rozkladem čísel v součin mocnin prvočísel: Jednak rozklad samotné grupy v direktní faktory a jednak jím určený rozklad prvku grupy v součin činitelů, vzatých z direktních faktorů.

V příkladě multiplikativní grupy kladných racionálních čísel byly jednotlivými, nerozložitelnými faktory direktního rozkladu vesměs nekonečné cyklické podgrupy (mocnin jednotlivých prvočísel), a bylo jich nekonečně mnoho. Jen o málo složitější je direktní rozklad multiplikativní grupy *všech* zlouků, tj. racionálních čísel, různých od nuly. Zde totiž přistupuje ještě jeden direktní a nerozložitelný faktor, cyklická grupa řádu 2, vytvořená číslem — 1.

Většině čtenářů je v podstatě znám jiný příklad direktního rozkladu grupy: aditivní grupa komplexních čísel $x + i.y$. (Nechť čtenáře nemate okolnost, že grupovým násobením je zde sečítání čísel!) Tato grupa se přímo definuje pomocí obou svých direktních faktorů, jimiž jsou dvě od sebe odlišné aditivní grupy reálných čísel, tvořené jednak tzv. reálnými částmi x, jednak tzv. imaginárními částmi y komplexního čísla $x + i.y$.

Poněkud obecněji je direktním rozkladem ve tři vzájemně rozlišené aditivní grupy reálných čísel dána aditivní grupa všech vektorů v prostoru $x.i + y.j + z.k$ (i, j, k jsou tzv. jednotkové vektory).

V obou posledních příkladech šlo o direktní rozklad ve faktory, které jsou dále direktně rozložitelné.

Je důležité zdůraznit, že rozklad *samotné grupy* v direktní faktory nemusí být nijak jednoznačný (v tom je obdoba s rozkladem celých *přirozených* čísel v mocniny prvočísel neúplná). Jestliže však již direktní faktory jsou určeny, potom je odpovídající rozklad prvků v součin činitelů, vzatých z jednotlivých direktních faktorů jednoznačně určen (v tom je úplná obdoba rozkladu *racionálních* čísel v mocniny prvočísel). Příklad direktního rozkladu ve dva direktně nerozložitelné faktory to objasní. Vezměme za rozkládanou grupu G multiplikativní grupu všech racionálních čísel tvaru 2^k3^h, tedy

čísel 1, 2, $\frac{1}{2}$, 3, $\frac{1}{3}$, 4, $\frac{1}{4}$, 6, $\frac{1}{6}$, 9, $\frac{1}{9}$, ... Za jeden faktor direktního rozkladu grupy G položme podgrupu $G_1 = (2^k)$ ($k = 0, \pm 1, \pm 2, \ldots$) (tj. nekonečnou cyklickou grupu vytvořenou všemi celými mocninami čísla 2). Za druhý faktor direktního rozkladu pak zřejmě můžeme vzít podobně (multiplikativní) grupu $G_2 = (3^h)$ všech čísel, vytvořených mocninami čísla 3 s celistvými mocniteli. Můžeme psát zřejmý direktní rozklad

$$G = G_1 \times G_2 = (2^k) \times (3^h)$$

s direktně nerozložitelnými faktory.

Za druhý direktní faktor k faktoru G_1 můžeme však vzít též např. grupu $G_2' = (6^r)$ ($r = 0, \pm 1, \pm 2, \ldots$) mocnin čísla 6. Neboť je

$$2^k 3^h = 2^{k-h} 2^h 3^h = 2^{k-h} 6^h$$

a rozklad čísla $2^k 3^h$ v součin mocnin čísla 2 a čísla 6 je jednoznačný. (Jestliže totiž je $2^r 6^s = 2^{r'} 3^{s'}$, pak je

$$1 = 2^{r-r'} 6^{s-s'} = 2^{r-r'+s-s'} 3^{s-s'}$$

a to značí, že $s - s' = 0$, $r - r' + s - s' = 0$, tedy $s = s'$, a z toho $r = r'$.) Máme tedy i další direktní rozklad $G = (2^r) \times (6^s)$ v idrektně nerozložitelné faktory. A přece různé direktní rozklady téže grupy v direktně nerozložitelné faktory jsou v jistém smyslu rovnocenné. O tom nás poučuje základní věta teorie direktního rozkladu grup, tzv. věta Remak-Schmidtova[28]). Tuto

[28]) Větu dokázali téměř současně a nezávisle na sobě německý matematik R. Remak (v r. 1911) a ruský matematik O. Schmidt (1913) — týž, který proslul jako sovětský polární badatel. Zobecnění věty Remak-Schmidtovy podal — mezi jinými — z našich matematiků V. Kořínek.

větu, která je protějškem k větě Jordan-Hölderově, podáme v poněkud zjednodušené formě:

Buďtež

$$G = G_1 \times G_2 \times G_3 \times \ldots \times G_n = \\ = G_1' \times G_2' \times \ldots \times G_m'$$

dva direktní rozklady grupy G v direktně nerozložitelné faktory $G_i (i = 1, 2, \ldots, n)$ a $G_j' (j = 1, 2, \ldots, m)$. Potom počet direktně nerozložitelných faktorů vobou rozkladech je týž, $n = m$, a ke každému faktoru G_i jednoho rozkladu existuje s ním isomorfní faktor G_j' druhého (direktního) rozkladu. Dokonce lze z jednoho direktního rozkladu pomocí druhého direktního rozkladu sestrojovat další direktní rozklady tak, že libovolné faktory jednoho direktního rozkladu nahradíme vhodnými faktory druhého direktního rozkladu.

Věta Remak-Schmidtova nám ovšem nezaručuje existenci direktního rozkladu libovolné grupy v nerozložitelné faktory. (V případech konečných grup je však existence alespoň jednoho direktního rozkladu v nerozložitelné faktory téměř zřejma: Stačí prostě rozkládat postupně jednotlivé faktory jakéhokoli direktního rozkladu tak dlouho, pokud se rozkládat dají. Vzhledem ke konečnosti grupy to jednou musí skončit u direktního rozkladu v nerozložitelné faktory.) Tato věta jen udává úzký vztah mezi jakýmikoli dvěma direktními rozklady téže grupy v nerozložitelné faktory, jestliže již rozklady máme. V předchozím příkladě grupy G všech čísel tvaru $2^k 3^h$ nám říká mj. to, že každý direktní rozklad grupy G v direktně nerozložitelné faktory tvoří dvě nekonečné cyklické grupy (podgrupy v G).

Obraťme se konečně ke třetímu hlavnímu způsobu, jakým v případě *konečných grup* sledujeme výstavbu složité grupy z jejich jednodušších podgrup. (I tato metoda má sice jisté rozšíření na nekonečné grupy, které se však daleko vymyká z rámce této knížky.)

Již jsme se zmínili, že nejjednoduššími konečnými grupami jsou grupy prvočíselného řádu, protože nemají vůbec žádných netriviálních podgrup. Pojem jednoduchosti vznikl rozšířením tohoto příliš úzkého pojmu jednoduchosti grupy: Grupa je jednoduchá, nemá-li netriviální normální podgrupy. Jiné rozšíření takové přílišné jednoduchosti grupy, jakou vidíme na grupách prvočíselného řádu, máme v grupách, jejichž řád je mocninou prvočísla p. To jsou tzv. p-grupy. Teorie p-grup se dosud nedá soustředit do jedné nebo několika málo jednoduchých vět, které by shrnovaly podstatné poznatky o věci; ostatně také výklad byť i jen základních výsledků teorie p-grup by si vyžádal zavedení mnoha pojmů, o nichž dosud nebyla řeč. Omezíme se proto na uvedení několika jednoduchých vlastností p-grup.

Předně jsou p-grupy zhruba řečeno příbuzné komutativním grupám, ale tato příbuznost se stává stále složitější, čím větší je mocnitel n v řádu p^n (p je prvočíslo) dané p-grupy. Tak nejen pro $n = 1$, nýbrž i pro $n = 2$ je každá p-grupa komutativní. (Tak např. třeba grupy řádu $13^2 = 169$ jsou komutativní.) Pro $n = 3$ již máme jen jistou slabou náhražku komutativity. (Ta spočívá v tom, že co nejmenší normální podgrupa taková, že faktorová grupa dle ní je komutativní, sestává právě ze všech prvků, které jsou komutativní s každým prvkem grupy; stručně se říká, že komutátorová podgrupa je rovna centru grupy.)

Z p-grup, které jsou stavebními kameny složitějších

grup, jsou důležité tzv. Sylowovy podgrupy dané grupy. Jsou to p-grupy s co největším mocnitelem n řádu p^n, které jsou obsaženy v dané konečné grupě. Teorie Sylowových podgrup vychází z pozoruhodného zjištění, že ke každé nejvyšší mocnině p^n prvočísla p, která je činitelem řádu dané konečné grupy, existuje Sylowova podgrupa řádu p^n.

Běží pak dále o to určit co nejblíže povahu dané konečné grupy z podmínek, kladených na její Sylowovy podgrupy. Tak např. jsou dokonale popsány typy isomorfismu konečných grup, jejichž Sylowovy podgrupy jsou cyklické grupy. Speciálně jsou tím odkryty všechny možné grupy, jichž řád obsahuje prvočísla vesměs jen v první mocnině. (Jako aplikace Galoisovy teorie rovnic pak vyplývá, že rovnice, jichž grupy mají vesměs cyklické Sylowovy podgrupy, se dají řešit pomocí šesti základních početních úkonů algebry.)

Tím uzavíráme zběžný pohled na způsoby, jakými se studuje v teorii grup budování složitějších grup z jednodušších podgrup.

Na ukončenou se obraťme alespoň k nejhrubšímu náčrtu jisté teoreticky důležité aplikace teorie grup, totiž aplikace na tzv. topologii. Jde o spojení teorie grup s vyšetřováním nejzákladnějších geometrických pojmů, které je stejně hluboké a obtížné jako překvapující.

Nejprve několik přibližných slov o tom, co je to topologie.

Topologie[29]) je od geometrie odštěpená teorie těch

[29]) Slovo topologie je z řeckého topos = místo a logos = = slovo, nauka. Dříve se užívalo termínu analysis situs — lat. rozbor uložení. Založena v podstatě francouzským matematikem H. Poincarém a holandským matematikem L. Brou-

základních vlastností geometrických útvarů, které zůstávají zachovány při jejich spojitých a vzájemně jednoznačných transformacích, chceme-li, deformacích. Podat přesnou definici pojmu spojité, vzájemně jednoznačné transformace, čili tzv. topologické transformace (deformace) není jednoduché. Spokojíme se zde s přibližným objasněním tohoto pojmu na názorných příkladech.

Mysleme si geometrický útvar, např. kruh v rovině z dokonale roztažitelného materiálu, např. na povrchu gumy. Gumu s nakresleným kruhem smíme jakkoli roztahovat, stlačovat, mačkat a podobně deformovat, jen nesmíme nikde gumu přetrhnout (tím by deformace přestala být spojitou) a nikde nesmíme dvě místa povrchu gumy spojit v jedno (slepit) (tím by deformace přestala být vzájemně jednoznačnou). Tak lze topologicky deformovat kruh v trojúhelník nebo čtverec, ale např. nikdy ne v úsečku nebo v mezikruží. Ať gumovou rovinu deformujeme topologicky jakkoli, vždy to, co vznikne z kružnice, bude nepřetržitá, do sebe uzavřená a sebe neprotínající čára (tedy např. to nikdy nebude osmička), která bude rozdělovat to, co topologickou deformací vzniklo z roviny, ve dvě souvislé plošné části: ve vnitřek a ve vnějšek toho, co takto vzniklo z kružnice.

Topologie je tedy exaktním rozborem toho, čemu v nejobecnějším a poněkud neurčitém smyslu slova

---

werem koncem minulého a začátkem tohoto století, stala se topologie jednou z nejdůležitějších základních teorií moderní matematiky. Z vynikajících současných topologů jmenujeme sovětské topology Alexandrova a Pontrjagina, z Američanů Alexandera a Lefschetze. Z našich současných matematiků podstatně přispěl k rozvoji moderní topologie E. Čech.

říkáme tvar, vzájemná poloha a spojitost bez ohledu na délky, šířky a vzdálenosti vůbec.

Abychom měli na očích alespoň jeden příklad topologické rovnocennosti a topologické odlišnosti ploch v prostoru, představme si obyčejný hliněný hrnec s jedním uchem před vypálením. Topologickou deformací jej můžeme převést až např. v těleso podoby prstence (tzv. anuloid). Tedy povrch hliněného hrnce s jedním uchem je např. topologicky rovnocenný s povrchem nafouklé duše pro jízdní kolo (včetně ventilku, který nic nemění na topologické povaze prstencovitého povrchu). Naproti tomu se nám nikdy nepodaří topologickou deformací uhnísť z hliněného hrnce s jedním uchem před vypálením kouli; stejně tak se nám ale nepodaří topologickým hnětením opatřit jmenovaný hrnec druhým uchem. Koule, hrnec s jedním uchem a hrnec se dvěma uchy jsou tělesa a mají povrchy topologicky odlišné. Koule je však topologicky rovnocenná s hliněným hrncem *bez ucha*, s krychlí, s trojbokým jehlanem. Hrnec s jedním uchem je topologicky rovnocenný s prstencem (anuloidem).

K vyšetřování topologických vlastností ploch, těles a obecnějších útvarů, i takových, které jsou uloženy v prostorech více než trojrozměrných, se užívá tzv. kombinatorické metody. Ta je právě oním mostem, který spojuje abstraktní pojem grupy s hlubokým rozborem našich nejzákladnějších geometrických tzn. topologických pojmů tvaru, rozprostření a (vzájemného) uložení a spojitosti. Pokusme se pochopit základní myšlenku kombinatorické metody na příkladě.

Představme si již zmíněný povrch prstence. Topologickou podstatu tohoto tvaru si dostatečně jasně uvědomujeme globálním prostorovým názorem. Avšak tento názor nás snadno může zavést na scestí svou

ohraničeností a povrchností, například již tehdy, máme-li na mysli složitým způsobem topologicky zdeformovaný povrch našeho prstence. Tím spíše se to může stát při topologicky složitých plochách nebo tělesech, kde globální názor selhává. Zde nutno k celkové topologické povaze plochy dojít jejím složením z vhodných topologicky jednoduchých částí; při tom topologický charakter útvaru vynikne ze způsobu, jakým spolu souvisí jednotlivé části. Naprosto nutný je pak takový kombinatorický postup při více než trojrozměrných útvarech, kde nám bezprostřední geometrický názor chybí vůbec. Mysleme si tedy na povrchu našeho prstence jakousi „dopravní síť", skládající se z konečného počtu bodů — jakýchsi dopravních uzlů (a zároveň jediných stanic) a ze „spojů", tj. na povrchu prstence vedených jednoduchých čar, spojujících nějakým způsobem tyto uzly. Sledováním cestovních možností v takových sítích dospíváme již k některým topologickým poznatkům o dané ploše. Neboť topologickou deformací plochy se sice mění vzdálenosti dopravních uzlů, křivosti, délky a vzdálenosti jednotlivých spojů, ale nevznikají ani nové dopravní uzly, ani nová dopravní spojení, a žádná dopravní spojení se tím neruší. Tak se projeví topologická rozdílnost povrchu našeho prstence od povrchu koule např. takto: Mysleme si na povrchu prstence jakýkoli z pevného dopravního uzlu vycházející a do něho se vracející cestovní okruh sestavený z jednotlivých spojů tak, že každým zvoleným uzlem (stanicí) se projíždí jen jednou. Pak ať si vyhédneme jakékoli dva další dopravní uzly (mimo zmíněný okruh), můžeme vždy buďto vyhledat anebo v nejhorším případě zavést nové spoje tak, abychom se dostali z jednoho do druhého uzlu, aniž dojde ke křižování, nebo aniž bychom dokonce měli kus společné dráhy s dříve vytčeným uzavřeným

cestovním okruhem. Naproti tomu na kouli to zřejmě možné není: Jakmile si zvolíme jeden bod uvnitř a druhý bod vně uzavřeného cestovního okruhu na povrchu koule, nedostaneme se po povrchu koule žádným způsobem z jednoho do druhého, aniž křižujeme daný do sebe uzavřený cestovní okruh, nebo aniž s ním máme část dráhy společnou.

Nyní jde o to, jak systematicky prozkoumat cestovní možnosti v takové dopravní síti na dané ploše. K tomu cíli si zvolme určitý bod (dopravní uzel a stanici) za východisko a po jakkoli složitém cestování v něm vždy naši cestu ukončíme. Tak vznikají tzv. uzavřené cesty, které jsou sledem na sebe navazujících spojů, při čemž je dán a zdůrazněn smysl postupu vpřed. Jinak nečiníme našemu cestování po ploše žádné omezení, takže můžeme jedním a týmž spojem nebo více spoji, nebo i částečným do sebe uzavřeným okruhem procházet vícekrát — ať již v původním nebo v opačném smyslu; můžeme speciálně projít týmž uzavřeným celým okruhem několikrát v jednom i opačném smyslu, můžeme se bezprostředně vracet do našeho východiska přesně po svých stopách — to vše budou uzavřené cesty. Pojem uzavřené cesty není tedy pouhým souhrnem prošlých spojů a stanic. Kdybychom chtěli názorně vyznačit naši výzkumnou (uzavřenou) cestu, učinili bychom tak způsobem, jehož s úspěchem použil antický hrdina Herakles v bludišti Minotaurově: Vyznačovali bychom naši pouť nití, kterou bychom po cestě odvíjeli, vyznačujíce smysl našeho postupu třeba pomocí pravotočivého předení nitě. Pak ovšem úseky, kterými jsme prošli několikrát, budou proloženy nití vícenásobně a v příslušném smyslu.

A nyní přijde to podstatné, co dovoluje užít pojmu grupy: Kdybychom si počínali přesně jako Herakles,

navíjeli bychom opět naši nit vždy pokud bychom se přímo a bez přerušení vraceli v nějaké části naší cesty přesně po vlastních stopách, obrátivše se v některé „stanici" čelem vzad. Pak by však více cestám odpovídala jediná tzv. redukovaná stopa. Všechny cesty by se nám tím rozpadly do tříd cest, při čemž do jedné a téže třídy bychom kladli cesty s touž redukovanou stopou.

Je přirozené považovat (z hlediska našeho cíle) uzavřené cesty s toutéž redukovanou stopou za rovnocenné? Je to přirozené a my to učiníme. Neboť nám nejde, jako o to šlo Heraklovi, o to, abychom se vrátili přesně po svých stopách, a tím se uchránili zbloudění. Nám jde naopak o to, abychom bludiště našich spojů probádali co do možnosti spojení a k tomu nám prosté cestování tam a zpět neustále ve vlastních stopách nepřispívá. Zvláště pak ty uzavřené cesty, jež se přesně po vlastních stopách vracejí do našeho východiska, nikde od nich neodbočujíce, budeme považovat za rovnocenné s „cestováním", při němž setrváváme v našem východišti. Za podstatně různé budeme považovat jen takové cesty, které zanechávají různé redukované niťové stopy, tak, jako dva zlomky považujeme za různé jen tehdy, když výsledky dělení čitatele jmenovatelem jsou různé.

A tím jsme u tzv. grupy uzavřených cest, lépe grupy tříd vzájemně neodlišných cest naší sítě, které se říká komplex drah.

Vskutku:

1. Každé dvě uzavřené cesty můžeme v daném pořadí „znásobit" tak, že navážeme jednu na druhou. Při tom nemůžeme dostat podstatně různé cesty, jestliže nebude alespoň jedna z obou znásobených cest nahrazena cestou od této podstatně různou. (To si snadno představíme, když si uvědomíme, že redukovaná niťová stopa součinu

obou cest se dostane tak, že prostě projdeme obě cesty v daném pořadí po sobě a redukujeme po způsobu Heraklově.) — První axiom jednoznačnosti a neomezenosti grupového násobení je splněn.

2. Druhý axiom teorie grup, axiom asociativity, je splněn téměř samozřejmě, jak si čtenář sám laskavě uvědomí.

3. Třetí axiom, axiom jednotkového prvku, je splněn rovněž téměř samozřejmě; jednotkou naší grupy podstatně různých cest je v podstatě cesta po východišti, neboli zanedbaná cesta tam a zpět ve vlastních stopách.

4. Konečně i axiom inversního prvku je splněn: inversní cestou k dané cestě je táž cesta s obráceným smyslem postupu.

Takovým způsobem se tedy objevuje pojem grupy jako nerozlučný pomocník kombinatorické topologie.

Vše matematicky podstatné z toho, co jsme zde vyložili obrazným způsobem lze ovšem vyslovit způsobem přesným a abstraktním, ale od toho tu upouštíme. Grupy cest, jež takto vznikají, jsou nekonečnými nekomutativními grupami, jež mají veliký význam pro teorii grup samotnou. Jsou to tzv. volné grupy; tímto názvem vyznačujeme přesně definovanou a tyto grupy charakterizující vlastnost, která — zběžně řečeno — značí, že prvky takové grupy jsou vzájemně vázány (pomocí grupového násobení) co nejslabšími vztahy, tj. jen takovými, které již nutně vyplývají ze splnění axiomů grupy.

Volné grupy cest jsou ovšem sotva počátkem kombinatorické topologie. Jsou oním základním schématem, které dovoluje vyjadřovat topologické vlastnosti ploch pomocí jistých rovností mezi prvky grupy cest, anebo lépe (což je ale logicky totéž) pomocí jistých, faktorových grup utvořených z grupy cest. Vlastním prostřed-

kem topologie jsou teprve tyto faktorové grupy. Nejdůležitější na věci je, že tyto faktorové grupy závisí jen na topologické povaze útvaru (např. plochy) a nikoli na soustavě cest, pomocí níž vznikly.

Tolik alespoň zhruba k naznačení, jak grupová zákonitost nabývá v kombinatorické topologii hlubokého významu geometrického. — Dodejme, že existují i jiné, snad méně názorné, ale pro většinu úkolů topologie jednodušší způsoby, jakými se objevují potřebné, plochu topologicky charakterizující faktorové grupy, jež sestrojujeme v grupě cest, pomocí zmíněných rovností. Tyto faktorové grupy, tzv. grupy Bettiho, jsou komutativními grupami, takže pro většinu zásadních úkolů topologie vystačíme s mnohem jednodušší teorií komutativních grup. (O tom se čtenář může poučit ve velmi přístupně psané knížce od znamenitého sovětského topologa Alexandrova.)

9. kapitola

ZÁVĚR

V předchozí, poslední kapitole našich výkladů o grupách, jsme se z dálky (dílem ze značné dálky, která dává bohužel splývat pevným obrysům), podívali na alespoň něco z toho, co jsme si na teorii grup a jejich užitích nestačili prohlédnout zblízka.

Neuškodí však také přehlédnout jediným krátkým pohledem za sebe tu cestu — tu malou počáteční část výstupu k teorii grup — kterou jsme skutečně prošli.

S pojmem grupy jsme se seznámili v jeho zvláště důležitě uskutečněné podobě grupy zákrytových pohybů. Vyzdvihnuvše typické vlastnosti skládání zákrytových pohybů (opět v zákrytové pohyby) ve tvar čtyř axiomů, shledali jsme, že takovouto zákonitostí, takovými vlastnostmi jsou obdařeny i četné jiné druhy skládání. To nás vedlo k obecnému, abstraktnímu pojmu grupy, jakožto souboru nějakých prvků, které lze po dvou „skládat" — říkali jsme: grupově násobit — tak, že jsou splněny axiomy 1—4.

Zároveň jsme byli vedeni k důležitému pojmu isomorfismu: dvě grupy platily za isomorfní, když měly nejen stejný počet prvků (prvky z jedné grupy se daly vzájemně jednoznačně zobrazit na prvky z druhé), nýbrž i tehdy, když skládání, zhruba řečeno, v obou probíhalo stejně, takže se dalo skládání v jedné grupě přenesením úplně nahradit skládáním podle gruhé grupy — a obráceně. Vyzdvihli jsme, že vlastním předmětem bádání

abstraktní teorie grup nejsou samotné (konkrétní) grupy, nýbrž hned celé typy grup navzájem isomorfních. Tím poučky abstraktní teorie grup nabývají největší možné obecnosti, obecné aplikovatelnosti (na každou jednotlivou grupu z grup vzájemně isomorfních, kdekoli by se vyskytla) a zároveň co největší přesnosti a jasnosti — ovšem to vše za cenu určité myšlenkové nesnadnosti pro toho, kdo není zvyklý myslet abstraktně.

Abstrakci, jak se ukázalo, je možno i nutno vyvažovat obráceným pochodem konkretizace a realizace abstraktních pojmů teorie grup. To bylo ukázáno především na isomorfní reprezentaci každé abstraktní konečné grupy, lépe řečeno: každého z možných typů isomorfismu konečných grup, konkrétní grupou číselných matic. (Byl předveden ovšem jen nejjednodušší, prakticky i teoreticky málo významný ukázkový způsob takové reprezentace.)

Věnovali jsme se dále několika více méně namátkou vybraným příkladům základních pouček abstraktní teorie grup a příslušných důkazových metod. Podali jsme také několik aplikací (v matematice), z nichž byl poměrně nejtěžší výklad a důkaz jednoduchosti alternujících grup stupně n.

A nakonec, po této námaze, jsme se podívali, jak již bylo řečeno, z dálky a zhruba na některé vyšší výsledky, úkoly a aplikace teorie grup.

OBSAH

ŠKOLA MLADÝCH MATEMATIKŮ

o grupách

LADISLAV RIEGER

Pro účastníky matematické olympiády
vydává ÚV Matematické olympiády
v nakladatelství Mladá fronta
Řídí akademik Josef Novák
Obálku navrhl Jaroslav Příbramský
Odpovědný redaktor Ladislav Smoljak
Publikace číslo 3396
Edice Škola mladých matematiků,
svazek 34
Vytiskl Mír, novinářské závody, n. p.,
závod 1, Praha 1, Václavské nám. 15
6,13 AA, 6,32 VA. 144 stran
Náklad 5500 výtisků. 2. vydání (v MF 1.)
Praha 1974. 508/21/82.5

23-041-74 03/2 Cena brož. výt. Kčs 8,50