O grupách a svazech

ESTA K VĚDĚNÍ

65

LADISLAV RIEGER

O grupách a svazech

PŘÍRODOVĚDECKÉ
VYDAVATELSTVÍ

CESTA K VĚDĚNÍ

65

LADISLAV RIEGER

O grupách a svazech

PŘÍRODOVĚDECKÉ
VYDAVATELSTVÍ

Dr. LADISLAV RIEGER

O grupách a svazech

Přírodovědecké vydavatelství, Praha

1952

Obálku navrhl a graficky upravil Miloš Hrbas

PŘEDMLUVA

V této knížce jsem se snažil jít ve stopách oněch svazečků sbírky „Cesta k vědění", které dobře plnily její hlavní poslání: nevelkým rozsahem uvádět do vyšších partií exaktních věd přírodních na podkladě nanejvýše vědomostí ze školy třetího stupně.

Při knížkách tohoto zaměření a takových předpokladů je ovšem 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 (theorie grup*) a vůbec ne, pokud je mi známo, v dobrých popularisujících publikacích. Do jaké míry se mi podařilo se s tímto problémem vyrovnat, to posoudí čtenáři.

V podstatě mi šlo o toto: seznámit čtenáře některými základními pojmy theorie grup a theorie svazů, které obě mají v současné matematice obdobný a základní význam. Ukázat na různorodém příkladovém materiálu, že běží v obou případech o velmi obecnou matematickou zákonitost, kterou jsme obje-

* V naší knižní literatuře je theorie grup zastoupena: „Úvodem do theorie grup" od prof. Borůvky (viz seznam literatury) — přes velikou vědeckou cenu a hloubku této publikace se mi zdá, že pro opravdu uvádějící seznámení s grupami to není vhodná publikace, a to jednak pro vysokou abstraktnost, jednak pro to, že značnou část knížky zaujímají útvary daleko obecnější, než grupy, t. zv. grupoidy, jimiž se prof. Borůvka zabývá ve svých odborných pracích. Čtenáři ovládajícímu základy theorie grup a cvičenému v abstraktním myšlení možno ovšem četbu Borůvkovy knížky vřele doporučit.

vili v nejrůznějších jejích konkretních tvarech, v matematice i přímo ve skutečnosti. Upozornit a pokud lze i ukázat na aplikace v přírodních a technických vědách. Předvést několik typických ukázek důkazových method. Naznačit úkoly obou theorií a alespoň v hlavních rysech ukázat některé další výsledky, jichž bylo dosaženo poměrně nedávno.

Tato knížka nemá být ani 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 algebraické theorie, jakými jsou theorie grup a svazů, nejsou samoúčelné abstraktní hříčky zasvěcených matematiků.

Kniha není určena pro odborníky; může je však přece jen zajímat stať o induktivním důkazu jednoduchosti alternující grupy stupně $\neq 4$.

Za účelem kontroly porozumění textu a pro prohloubení a doplnění výkladu samostatným uvažováním jsou k většině paragrafů připojena cvičení. Méně snadná jsou opatřena hvězdičkou, případně zběžným návodem k řešení.

K ilustraci a objasnění abstraktních pojmů přispějí jistě i obrázky. Nakreslil je dle mých návrhů asistent Jos. Matušů z matematického ústavu vysoké školy strojního inženýrství v Praze.

Lad. Rieger

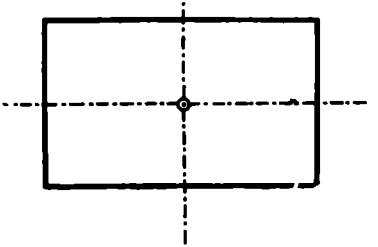
ČÁST I.

THEORIE GRUP

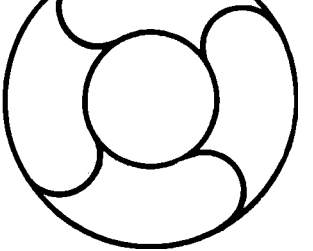
1,1. POJEM ZÁKRYTOVÉHO POHYBU

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 t. zv. *zákrytové pohyby*, jimiž se ztotožní útvar jako celek sám se sebou, aniž se tedy obecně jeho jednotlivé body vrátily do svých původních poloh. Vystižení geometrické pravidelnosti útvaru je potřebí tedy hledat v souhrnu jeho zákrytových pohybů. Tak na př. obdélník (obr. 1) má tři takové zákrytové pohyby, t. j. dvojí překlopení (dle každé z obou os souměrnosti) a jejich kombinaci,



Obr. 1.

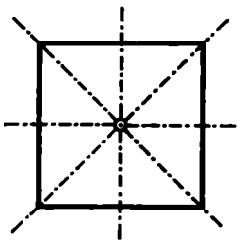


Obr. 2.

t. j. otočení o 180°. Útvar na obr. 2 má rovněž přesně tři zákrytové pohyby, ale jiné, totiž otočení roviny o 1, 2, 3 pravé úhly. Nekonečný pás na obr. 3 má nekonečně mnoho 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. 3.

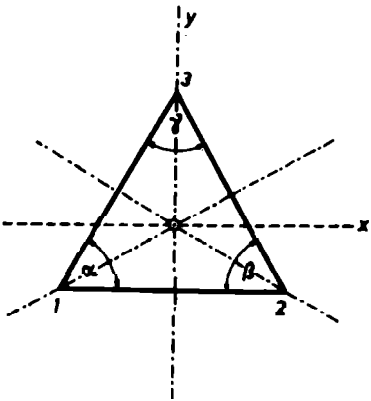
Aby později nevzniklo nedorozumění, je dobře výslovně objasnit geometrický ráz pojmu zákrytový pohyb. Na rozdíl od skutečného (fysikálního) pohybu při zákrytovém pohybu nepřihlížíme ani k časovému průběhu pohybu (k rychlosti), ani k tomu, po jaké dráze se jednotlivé body (geometricky pravidelného, tuhého) 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 na př. 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 na př. 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.)



Obr. 4.

Souhrn zákrytových pohybů libovolného daného útvaru má některé důležité a jednoduché základní vlastnosti. Tak na př. 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) a pod. 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 theorie geometrické pravidelnosti. Tak jsme vedeni k pojmu grupy zákrytových pohybů, kterýmžto názvem označme prozatím zhruba souhrn zákrytových pohybů daného útvaru vzhledem k tomu, jak se zákrytové pohyby skládají. Tento pojem si objasníme blíže pomocí příkladu zákrytových pohybů rovnostranného trojúhelníka.



Obr. 5.

Cvičení k 1,1.

1. Určete zákrytové pohyby: a) pravidelného šestiúhelníka, b) vlnovky $y = \sin x$, c) neomezené čtverové 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?).

1,2. GRUPA ZÁKRYTOVÝCH POHYBŮ ROVNOSTRANNÉHO TROJÚHELNÍKA. AXIOMY GRUPY.

Abychom mohli sledovat skládání zákrytových pohybů rovnostranného trojúhelníka (obr. 5)[1] vyznačme si pro jedno-

[1] Čtenář učiní dobře, když si vystřihne z papíru rovnostranný troj-

duchost 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 pojmenovali všech 6 zákrytových pohybů rovnostranného trojúhelníka, jak se čtenář sám snadno přesvědčí. Smluvme si ještě (jednou provždy), že zákrytový po-

	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.

hyb, 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. 1), jejíž správné sestrojení nechť si čtenář ověří (viz pozn. 1).

úhelník (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.

Její užití je zřejmé: výsledek CD na př. otočení o 120°, t. j. pohybu D, následovaného překlopením kolem osy úhlu γ, t. j. pohybem C, najdeme v průsečíku řádku uvedeného písmenem D a sloupce, uvedeného písmenem C, tedy odečteme $CD = B$ výsledek je překlopení kolem osy úhlu β; podobně $AB = E$, $AA = A^2 = J$ atp.

Pomocí tabulky 1 lze nyní pohodlně určovat i výsledné 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 čísla lomená (čili racionální čísla)), t. j. formulujeme 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, t. j. 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 na příklad jako

[2]) Zapisování po sobě následujících pohybů od prava doleva má svoje důvody, jež se objasní při definici „násobení“ permutací a transformací v odst. 1,3. Je důležité si na to zvyknout.

1,2 nebo číslo S je dáno jako $\frac{5-2+3}{50}$ 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 na př. 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 zákrytové 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 $L \neq 0$) máme jedno jediné číslo $\frac{1}{L}$, t. zv. převrácenou hodnotu k L, t. j. číslo, jež znásobeno daným číslem dá jednotku, $L \cdot \frac{1}{L} = 1 = \frac{1}{L} \cdot L$. (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", t. j. je též

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

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

Tomu, že 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 $X = Y^{-1}Z$. Na př. 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, t. j. 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 jsou právě tím, co mají všechny úplné soubory zákrytových pohybů kteréhokoli geometricky pravidelného útvaru společné. Pojem grupy (zákrytových pohybů) tedy vystihuje matematickou podstatu pojmu pravidelnosti útvarů (prostorových i rovinných). Viděli jsme však také, že grupové axiomy jsou splněny právě tak i pro násobení (kladných lomených) čísel místo skládání pohybů, 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 rovněž grupu*, t. zv. násobící (čili multiplikativní) grupu kladných lomených čísel.

Je však ještě jeden (početní) zákon (axiom), který je splněn pro násobení čísel a není splněn na př. pro skládání zákrytových pohybů rovnostranného trojúhelníka, totiž t. zv. 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 na př. 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 násobící grupa kladných lomených čísel je *komutativní grupa*, také někde: *Abelova*[3] grupa, kdežto grupa zákrytových pohybů rovnostranného trojúhelníka není komutativní.

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

Říkáme, že násobící grupa kladných lomených čísel je nekonečná,[4] 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 $a, a^2, a^3, \ldots$ Naproti tomu libovolný zákrytový pohyb X trojúhelníka rovnostranného proveden šestkráte po sobě dá identický pohyb, t. j. zde platí bez omezení rovnost $X^6 = J$, takže $X^7 = X$, $X^8 = X^2, \ldots$ — „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 si právě uvedli, si tedy uvědomujeme tento souhrnný poznatek: *Některé* základní početní zákony, totiž t. zv. zákony grupové (1) až (4), samozřejmě

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

[4] O rozlišování různých nekonečen se čtenář poučí v knížce této sbírky B. Pospíšil: *Nekonečno v matematice*; tam zjistí, že všech kladných lomených čísel je spočetně nekonečně mnoho (tolik kolik celých kladných čísel) — jejich grupa je tedy, jak se říká spočetně nekonečná.

splněné při násobení (kladných lomených, př. 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 nemusí 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 (t. j. 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, jako je *A. Speiser*[5] 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 theorie grup, tato základní disciplina abstraktní algebry. Bez obšírných výkladů je předně pochopitelné, že různé úlohy z ornamentální geometrické výzdoby (ať již plošné nebo prostorové) jsou v podstatě úlohami theorie 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.

Theorie konečných grup (zákrytových pohybů) je dále podstatným pomocníkem nauky o t. zv. pravidelných mnohostěnech vepsaných do koule. (Stručné odvození tvaru pravidelných mnohostěnů pomocí theorie grup najde čtenář na př. v učebnici Zassenhausově.[6]

[5] Srov. jeho *Theorie der Gruppen endlicher Ordnung.*

[6] H. Zassenhaus, *Lehrbuch der Gruppentheorie.*

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

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

Cvičení k 1,2.

1. $ABCD = ?$, $ABDE = ?$, $A^2B^2 = ?$ Řešte rovnice $AX = E$; $XE = B$, $XB = X^3C$.

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

3. $A^{15} = ?$, $D^{-135} = ?$, $(AD)^{15} = ?$ (Návod: na př. $D^3 = J = D^0$ a pod.; 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 $(XY)^n \neq X^n Y^n$.)

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

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

1,3. OBECNÝ POJEM GRUPY. JINÉ PŘÍKLADY GRUP.

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

[7] Bližší v učebnici Speiserově nebo ve speciální monografii od F. Burckhardta (viz lit. na konci).

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

dalších podobách nalézáme splněny tytéž axiomy grupy (1) až (4) z 1,2. K tomu si výslovně uvědomme následující. Axiomy grupy budou splněny vždy nějakým, násobení připomínajícím úkonem, na př. „skládáním" (pohybů) prováděným s předměty, kterým budeme od nynějška říkat *prvky grupy*. Tyto prvky musí ovšem tvořit vymezený soubor (t. j. *grupu*) tak, že výsledek „násobení" („složení") dvou prvků grupy v daném pořadí je opět prvkem grupy. Chceme-li si tedy výslovně formulovat axiomy grupy obecně, vrátíme se do předchozího odstavce 1,2 a slova „zákrytový pohyb" nahradíme slovy „prvek grupy", slova „zpětný pohyb", slovy „inversní prvek", slova „identický pohyb" slovy „jednotkový prvek", nebo i stručněji „jednotka" a konečně slova skládání „pohybů" slovem „násobení". Musíme však mít stále na paměti, *že slovo jednotka a slovo násobení* (přesněji řečeno: jednotka grupy, grupové násobení (v grupě) *a odpovídající názvy, jako součin, mocnina* (s celistvým mocnitelem) *mají od nynějška pro nás obecný smysl*, že to může být cokoli, na co se vztahují zákony (axiomy) grupy, v daném případě tedy také to, co s násobením čísel nemá co dělat). Abychom to ozřejmili hódně drastickým způsbem, připomeňme si, že rovněž *sečítání* čísel, na př. celých, kladných i záporných včetně nuly *tvoří grupu*, t. zv. *sečítací* (čili aditivní) *grupu celých čísel*. Zde se „násobením" grupy rozumí obyčejné sečítání, jednotkovým prvkem je obyčejná nula a inversním prvkem k celému číslu a je číslo $-a$. Sečítací grupa celých čísel je tedy komutativní (Abelova) nekonečná grupa; axiomy grupy (1), (2), (3), (4) a (5) jsou tu známými základními početními zákony pro sečítání. (Podobně je tomu ovšem pro lomená nebo i reálná čísla.)

Možná, že se čtenář zeptá, proč se tedy neužívá pro úkon ve smyslu axiomů grupy názvosloví, vzatého ze sčítání, místo z násobení nebo vůbec nějakého jiného „neutrálního" názvosloví. Skutečně někteří američtí matematikové užívají t. zv. sečítací (aditivní) symboliky a názvů i pro některé nekomutativní grupy, ale všeobecně to není přijímáno. Jak z formálních důvodů jednoduchého psaní, tak i vzhledem k t. zv. representacím grup grupami matic (o tom viz

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

Pojem a theorie geometrické pravidelnosti, z nichž jsme vyšli, se jeví s obecného stanoviska, na něž hodláme vystoupit, jako zcela speciální aplikace abstraktní theorie 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 $1, 2, 3, \ldots, n$. Jestliže zastoupíme 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 na střední škole spojujeme se slovem permutace (n čísel) jen představu 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. Na př.

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

značí totéž co rovnosti

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

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

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).[9] Na př. je-li

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

a

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

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

pak

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

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

(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 t. zv. identickou permutací (čti jota)

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

(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 $n! = 1 \cdot 2 \cdot 3 \ldots n$ (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 theoreticky i v aplikacích, v matematice i v přírodě. Lze říci, že v moderní matematice na poč. XIX. století se pojem grupy objevil v grupách permutací, a to přímo v aplikaci na theorii algebraických rovnic libovolného celistvého kladného stupně o jedné neznámé. (O této t. zv. *Galoisově*[10] theorii rovnic najde čtenář zmínku ve Schwarzově knížce „O rovnicích", v této sbírce „Cesta k vědění"; pro základní pojmy Galoisovy theorie viz na př. Kurošovu učebnici.)

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

V theoretické fysice nalézáme aplikace theorie symetrické grupy v kvantové mechanice,[11] kde jde o permutace elektronů v atomu či molekule.

Příklad 2. Grupa geometrických transformací.

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

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

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

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

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

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

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

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

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

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''.)[13]

Skládání euklidovských pohybů roviny lze tedy stručně vystihnout rovností

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

(Podobně jako při násobení permutací zaznamenáváme v součinu dvou geometrických transformací postup skládaných pohybů od prava doleva; hlubším důvodem pro toto nezvyklé psaní je okolnost, že zobecnění pojmu permutace na nekonečné soubory předmětů, jako jsou na př. body roviny, zahrnuje v sobě i pojem geometrické (euklidovské) transformace roviny jako zvláštní případ. Permutovanými předměty jsou pak na místě celých čísel páry reálných čísel (kde prvé číslo je úsečkou, druhé pořadnicí bodu) a euklidovský pohyb jakožto předepsané nahrazení starých souřadnic bodu, t. j. páru x', y' novými souřadnicemi téhož bodu, t. j. párem x, y, se opravdu jeví jako jistá „permutace" bodů roviny, rozumí se ovšem nikoli ve středoškolském, nýbrž ve shora uvedeném smyslu slova.)

Snadno se dá ukázat,[14] že euklidovské pohyby možno považovat za prvky grupy, že totiž platí i pro skládání euklidovských pohybů, považované za „násobení", v t. zv. *grupě euklidovských pohybů* roviny, axiomy (1) až (4). Tato grupa je nekomutativní a nekonečná. (Neplatnost komutativního zákona již při obrácení sledu čistého posuvu a čistého otočení zná každý, kdo ví, že vpravo v bok a pak krok vpřed dá něco jiného, než krok vpřed a pak vpravo v bok.)

Ke grupě euklidovských pohybů roviny (včetně překlápění) můžeme dospět i jiným, méně názorným způsobem: Je to totiž právě

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

[14] Přenechávám to čtenářově 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.)

ta grupa (t. zv. lineárních transformací či permutací) bodů[15] roviny, která zachovává vzdálenost dvou bodů, což vychází na požadavek, aby dva body x_1, y_1 a x_2, y_2 vždy přešly ve dva body x_1', y_1' a x_2', y_2' tak, že

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

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

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

Ve fysice poznáme význam obecné theorie grup transformací s daným invariantem na tomto příkladě: Z požadavku speciální theorie relativity, že světelný signál se má šířit stejnou a nepřekročitelnou rychlostí na všechny strany nejen vzhledem ke zdroji světla (což je samozřejmé) nýbrž i v soustavě, která se vzhledem ke zdroji pohybuje přímočaře rovnoměrně, vyplývá (v nejjednodušším případě posuvu osy x v sobě) požadavek invariance (neměnnosti) funkce $x^2 - c^2t^2$ (při lineární transformaci starých „souřadnic" novými); „souřadnice" t má tu význam času, c značí rychlost světla. Tímto invariantem je definována jistá lineární grupa (neeuklidovských) transformací, t. zv. grupa *Lorentzova*. Její studium je matematickým základem speciální theorie relativnosti.[16] (Viz cvič. 10 k par. 1,4.)

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):

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

[16] Čtenář se může poučit o theorii relativity v přístupně psané knížce Fr. Závišky, nezapomenutelného profesora theoretické fysiky na KU, umučeného nacisty. Knížka má název *„Einsteinův princip relativnosti a theorie gravitační"*, vyd. JČMF.

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

Pak euklidovského otočení zní

$$x = a_{11}x' + a_{12}y',$$
$$y = a_{21}x' + a_{22}y'.$$

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

$$x = a_{11}x' + a_{12}y' + a_{13}z',$$
$$y = a_{21}x' + a_{22}y' + a_{23}z',$$
$$z = a_{31}x' + a_{32}y' + a_{33}z',$$

kde pevné číslo (t. zv. 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; na př. a_{13} je kosinus úhlu mezi starou polohou osy x-ové s novou polohou osy z-ové.)

Euklidovská otočení roviny, resp. prostoru jsou příklady t. zv. lineárních homogenních[17] transformací. Tímto pojmem, který má velikou důležitost v celé matematice, geometrii a i v theoretické fysice, rozumíme obecně souhrn závislostí n závisle proměnných čísel $x_1, x_2, \ldots, x_n$ 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 t. zv. řádkového indexu i a t. zv. sloupcového indexu k) plně určují svým souhrnem takovou lineární

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

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, t. j. 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 t. zv. determinant soustavy byl číslem od nuly různým.[18])

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 t. zv. 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 lin. hom. transformace.[19]

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

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

Složenou transformací AB (čili součinem AB obou transformací) rozumíme vyjádření závisle proměnných x_1, x_2, x_3 transformace A nezávisle proměnnými x_1'', x_2'', x_3'' transformace B, což se provede dosazením za x_1', x_2', x_3' z rovnic pro B

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

[19] Číselné příklady najde čtenář níže — zde by však pravidelnost skládání transformací spíše zatemnily, než objasnily.

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

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

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

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

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

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

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

Matici (stupně n), mající v i-tém řádku a k-tém sloupci číslo (a_{ik}), pak označujeme stručně jako (a_{ik}) (je-li záhodno, s dodatkem $i, k = 1, 2, 3, \ldots, n$).

Součinem matice $A = (a_{ik})$ násobené zprava maticí $B = (b_{ik})$ rozumíme tedy matici $AB = C = (c_{rs})$, kde

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

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

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

Jednotkovým prvkem je tu t. zv. jednotková matice

$$\begin{pmatrix} 1\,0\ldots 0 \\ 0\,1\ldots 0 \\ \ldots\ldots \\ 0\,0\ldots 1 \end{pmatrix}$$

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 $b_{11} = b$ a pod.) Násobení matic je prostě násobení čísel. Příslušné homogenní transformace jsou ty nejjednodušší lineární závislosti, řekněme

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

a pod.

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

b) Položme $n = 2$. Nechť na př.

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

Pak

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

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

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

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

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

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

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

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

Abychom se případně zbytečně nenamáhali, je dobře vyzkoumat, zda napsané rovnice mají vůbec řešení (pro každé x_1, x_2, x_3). Vidíme však, že přičteme-li k dvojnásobku první rovnice druhou rovnici, dostáváme rovnost $2x_1 + x_2 = 0$. To je v rozporu s libovolnou volitelností a tedy se vzájemnou nezávislostí proměnných x_1 a x_2. Lze tedy napsané rovnice řešit dle čárkovaných neznámých jen tehdy, jestliže je splněna podmínka $2x_1 + x_2 = 0$ (což obecně není), takže inversní transformace k transformaci o dané matici A neexistuje; matice A není regulární a není tedy prvkem naší grupy (lineární grupy matic stupně 3 s racionálními koeficienty). (Čtenář, znalý základů theorie determinantů to ví předem, neboť si všimne, že determinant dané matice A je nula, protože druhý řádek matice je -2-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, t. j. 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 idealisovaných barev.

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

Předpokládejme tři základní barvy v základní síle, t. j. modř M, červeň $Č$ a žluť $Ž$ tak, že smíšením těchto tří barev vznikne čirá (neutrální) barva N. K přibližné realisaci poslouží známý barevný kotouč, rozdělený na tři stejně veliké výseče, modrou, červenou, žlutou, na němž se dojem neutrální, ve skutečnosti šedivě špinavé směsi N docílí rychlým otáčením. Mísením základních tří barev lze (theoreticky) docílit všech barevných odstínů jen tehdy, když jsou základní intensity modré, červené a žluté dosti jemné. Mísení barev, ovšem v příslušné idealisaci, podléhá zákonům komu-

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

Příklad 5. Booleova grupa.

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

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

Této grupě, která je Abelova a při n daných předmětech má 2^n prvků, to jest skupin z daných předmětů, a která při nekonečně mnoha daných předmětech je ovšem nekonečná, se říká *Booleova*[20] grupa.

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

Cvičení k 1,3.

1. Upravte na „normální tvar"

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

permutace

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

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

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

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

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

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

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

---

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

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

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

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

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

kde c je konstanta, v je parametr, $|v| \leqq |c|$ tvoří grupu, t. zv. Lorentzovu grupu speciální theorie relativity. ($c \doteq 3 \cdot 10^9$ cm/sec je stálá rychlost světla ve vakuu, x, t jsou délka a čas (v cm a sec) na relativně klidné přímce a; x', t' jsou délka a čas na relativně pohybované přímce a' rychlostí v (stálou) a rovnoběžnou s přímkou a.[21]

1,4. POJEM ISOMORFISMU GRUP. ABSTRAKTNÍ POJETÍ GRUPY (TYP ISOMORFISMU).

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

[21] Srov. F. Záviška, *Einsteinův princip relativnosti a theorie gravitační*, JČMF Praha 1925, str. 60.

matic, mísením barev, shrnováním předmětů ze dvou skupin do jedné, pokud se nevyskytují v obou.

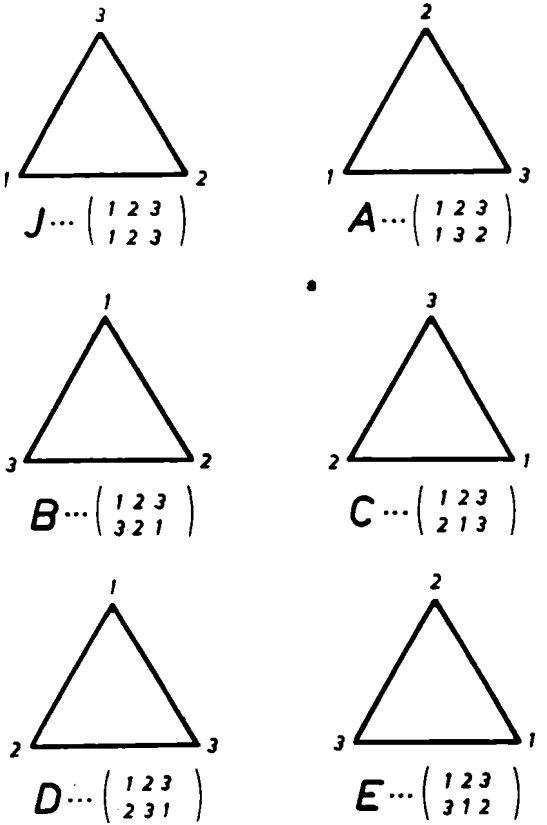
Stává se však, že dvě grupy, ačkoli se liší vzájemně buď ve svých prvcích, (některých či ve všech) anebo ve způsobu, resp. výsledcích grupového násobení, anebo v obojím, přece jsou *téhož typu*, čili, jak se říká, jsou *isomorfní* (z řec. iso = stejně, morfos = tvar). Pojem isomorfismu grup si dříve 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 odst. 1,2. 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 permutaci 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 trojúhelníka odpovídajícími permutacemi, pak jsme tím již zastoupili i každý součin (výsledek složení) pohybů součinem permutací, odpovídajících po řadě daným pohybům. Tak na př. 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 $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$. $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ je permutace odpovídající překlopení kolem osy úhlu β, $B = A \,.\, E$ (viz tab. v 1,2 a obr. 6).

Vidíme tedy, že symetrickou grupu permutací $\mathfrak{S}_3$ můžeme od grupy zákrytových pohybů rovnostranného trojúhelníka odlišit jen konkretní povahou prvků (jednou pohyby roviny trojúhelníka, po druhé permutace) a různým způsobem, ja-

kým 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



Obr. 6.

typu naší grupy všech permutací tří předmětů, čili typu grupy všech zákrytových pohybů rovnostranného trojúhelníka, a to pomocí příkladů 2 a 3 z odst. 1,3.

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

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

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

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 překlopením 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 odst. 1,2), 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. 1 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 *násobící* grupa všech *kladných* reálných čísel, druhá grupa budiž *sečítací* 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 klad-

ného 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 (na př. násobící grupy kladných reálných čísel) na jinou grupu (na př. sečítací grupu všech reálných čísel) nemusí být jen jedno, neboť právě takový isomorfismus dává i logaritmování při jiném, třeba při t. zv. 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, t. zv. 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

$$f(x_1x_2) = f(x_1) \cdot f(x_2)$$

(jestliže součin v G vyznačujeme prostým psaním činitelů vedle sebe a součin v H kvůli rozlišení vyznačujeme tečkou mezi činiteli).

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 násobící grupa kladných reálných čísel, G byla sečítací 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 gru-

pách) 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 theorie grup, který nutí k jasnému zavedení a využití pojmu isomorfismu.

Abstraktní theorie grup se tedy nezabývá určitou konkretní grupou (jako na př. je grupa permutací daného počtu předmětů nebo grupa matic s reálnými koeficienty daného stupně), nýbrž formuluje svoje poučky tak, aby platily pro všechny konkretní, 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 theorie 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 na př. na násobení permutací nebo násobení matic), tak i od samotného druhu prvku 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 konkretní grupy, tedy vlastnost či vztah, které do vlastní theorie grup nepatří.

Pro typ isomorfismu grup je tedy podstatný 1. počet jejich prvků (v příslušném zobecnění i na t. zv. nekonečný počet čili mohutnost množství prvků grupy, o tom viz Pospíšil, cit. v pozn. 3), 2. okolnost, že ke každým dvěma prvkům grupy v daném pořadí je (nějak) stanoven jednoznačně je-

jich součin podrobený axiomům (1) až (4), lhostejno, jakým způsobem se násobení uskuteční.

Smysl popsané abstrakce v theorii grup je dále v tom, že abstraktní theorie grup, nepřestávajíc na abstraktním zevšeobecňování vlastností známých konkretních grup systematicky hledá všechny typy grup, které jenom (po př. 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 (po případě zatím) v přírodě nebyly nalezeny, ale mají pro poznání dané přírodní zákonitosti důležitý význam theoretický (jehož praktický dosah se musí dříve či později objevit).

Cvičení k 1,4.

1. Dokažte, že násobící grupa všech komplexních čísel $\neq 0$ (tvaru $x + iy$) je isomorfní s násobící 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 sečítací grupou celých čísel. (Udejte přesně isomorfní zobrazení.)

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

4.*Ukažte, že Booleova grupa z par. 1,3 a grupa ze cvič. 8* (za týmž par.) jsou isomorfní grupy (při stejném počtu daných předmětů). (Isomorfní zobrazení přiřazuje skupině předmětů jakožto prvku jedné grupy skupinu všech zbývajících předmětů jakožto prvek druhé grupy.)

1,5. GRUPOVÁ SCHEMATA (TABULKY). ISOMORFNÍ REPRESENTACE 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 theorie grup) opřít o zákonitosti ve čtverečném schematu z prvků grupy, jehož zápisem je grupová tabulka (jak jsme ji poznali již v odst. 1,2), 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 t. zv. 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, na př. 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: $a^{n+1} = a^n \cdot a = j \cdot a = a, a^{n+2} = a^2, \ldots$ což lze znázornit na kružnici.) Číselným případem cyklické grupy řádu n je násobící grupa n-tých odmocnin z 1, což jsou ovšem obecně čísla komplexní.

Tabulka 5 předvádí t. zv. Kleinovu grupu; je to komutativní grupa řádu 4, daná na př. věcmi 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.

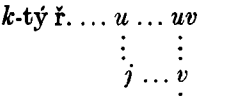
Jaké vlastnosti takového čtverečného schematu o n^2 polích obsazených n různými věcmi jsou typické pro grupová schemata? Odpověď, kterou podáme v následující větě, dává možnost studovat abstraktní typy isomorfismu konečných grup pomocí jisté konečné kombinatoriky čtverečných uspořádání n různých předmětů.

Věta 1.

Čtvercové schema o n^2 polích, zaplněných n různými předměty $j, a, b, c, \ldots$ — při čemž předmět j nechť leží v levém horním rohu — představuje grupu s jednotkovým prvkem j (v našem smyslu, t. j. tak, že za grupový součin xy libovolného 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 schema 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 $u \cdot v$).* (2) je t. zv. obdélníkové pravidlo, znázorněné tímto výsekem z tabulky:



Důkaz:

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

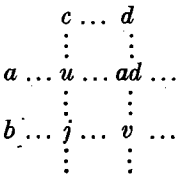
Za prvé tedy nechť j je jednotkový prvek a $a, b, c, \ldots$ ostatní prvky grupy, z nichž je tvořeno čtverečné schema znázorněné tabulkou.

Vlastnost (1):

Kdyby se jistý prvek grupy, na příklad a, vyskytoval v řádku, uvedeném třeba prvkem b dvakrát, jednou pod prvkem c a jednou pod prvkem d, pak by to znamenalo, že $b \,.\, c = b \,.\, d = a$. 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 schematu v poloze, vyznačené nejlépe tímto výsekem z tabulky:



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

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

Za druhé, nechť čtverečné schema 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:

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

(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 schematu 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 (t. j. z předmětů vystupujících ve zkoumaném schematu), 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 okem viditelné rozměry) 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 užití jiných prostředků, totiž hlavně t. zv. representace 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 representace abstraktní grupy grupou konkretní, 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 theorie 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 konkretních grup; při tom musíme ovšem pro toto isomorfní uskutečnění a vystižení čili *representaci* abstraktního grupového násobení konkretním grupovým násobením zvolit takové representující násobení, které je *universální*, aby každé grupové násobení se jím dalo vystihnout a za pomoci isomorfismu nahradit. Takovým universálním grupovým násobením je právě *násobení permutací* a ještě lépe: *násobení matic*. (Viz př. 1 a 3 v odst. 1,3.)

Druhým důvodem, který vlastně doplňuje a vysvětluje první, je opora, kterou nám v theorii 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 na příklad viděli v isomorfním vystižení grupy zákrytových pohybů rovnostranného trojúhelníka a zároveň symetrické grupy $\mathfrak{S}_3$ stupně 3 v předchozím odstavci.

Číselných vztahů při representaci grup maticemi využívá ke studiu abstraktně pojatých (representovaných) grup t. zv. *theorie charakterů*, o níž se čtenář poučí ve Speiserově učebnici theorie

grup; po př. ve speciálních monografiích (pro hlubší studium) od *D. E. Littlewooda*[22] a pro zvláštní nekonečné, t. zv. topologické grupy ve skvělém díle *L. S. Pontrjagina*.[23]

Konečně třetí, ovšem nikoli nejméně důležitý důvod k hledání isomorfní representace grup grupami matic, jsou aplikace fysikální a jiné, o nichž již byla zmínka a na něž (s příslušnou udanou literaturou) čtenáře nutno odkázat.

Než se obrátíme k isomorfním representacím, 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 sečítací grupy všech racionálních čísel (zlomků); tato grupa sama je podgrupou sečítací 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.

[22] D. E. Littlewood, *The theory of group characters and matrix representations of groups*, Oxford 1940.

[23] L. S. Pontrjagin, *Nepreryvnye gruppy*, ONTI NKTP SSSR 1938. (Vyšlo i v angl. př.)

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 prvků 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, z odst. 1,3) 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 konkretnost) 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 odst. 1,4.) Pozor na to, že symetrická grupa permutací n předmětů, která sama má $n!$ prvků, to jest permutací, může být tedy isomorfně representována 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 (permutace 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, t. j. 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

$$\begin{aligned}
X_1 &= 0 \,.\, X'_1 + 0 \,.\, X'_2 + \ldots + 1 \,.\, X'_{\pi^{-1}(1)} + \ldots + 0 \,.\, X'_m \\
X_2 &= 0 \,.\, X'_1 + 0 \,.\, X'_2 + \ldots + 1 \,.\, X'_{\pi^{-1}(2)} + \ldots + 0 \,.\, X'_m \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_m &= 0 \,.\, X'_1 + 0 \,.\, X'_2 + \ldots + 1 \,.\, X'_{\pi^{-1}(m)} + \ldots + 0 \,.\, X'_m
\end{aligned}$$

(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

$$\begin{aligned}
X'_1 &= 0 \,.\, X_1 + 0 \,.\, X_2 + \ldots + 1 \,.\, X_{\pi(1)} + \ldots + 0 \,.\, X_m \\
X'_2 &= 0 \,.\, X_1 + 0 \,.\, X_2 + \ldots + 1 \,.\, X_{\pi(2)} + \ldots + 0 \,.\, X_m \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X'_m &= 0 \,.\, X_1 + 0 \,.\, X_2 + \ldots + 1 \,.\, X_{\pi(m)} + \ldots + 0 \,.\, X_m .)
\end{aligned}$$

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 $a_{i\pi^{-1}(i)} = 1$ a $a_{ik} = 0$ pro $k \neq \pi^{-1}(i)$ a podobně permutaci ϱ matice (b_{rs}) s $b_{r\varrho^{-1}(r)} = 1$ a $b_{rs} = 0$ pro $s \neq \varrho^{-1}(r)$

$(i, k, r, s = 1, 2, 3, \ldots, m)$. Znásobením obou matic obdržíme (dle odst. 1,4) 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).

Neboť dle věty 2 lze každou grupu isomorfně representovat vhodnou grupou permutací a dle věty 3 tuto grupu permutací lze opět isomorfně representovat grupou matic; je tím tedy i dána isomorfní representace dané grupy grupou matic.

Věty 3 a 4 mají spíše theoretický, než praktický význam: Zaručují hledanou universálnost 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 sečí-

tání, odčítání, násobení a dělení čísel. Avšak representace ve smyslu věty 4 vede na matice zbytečně vysokého stupně, totiž rovného řádu grupy. Prakticky, pro studium struktury dané grupy, mají větší význam representace 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 theorii grup. Prostý příklad takové úsporné a účinné representace 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 předchozím odstavci.

V dalším opustíme pojem isomorfní representace, abychom alespoň z dálky ukázali, jakým způsobem řeší abstraktní theorie 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 t. zv. obecné theorie grup.

Zvláště významný je jmenovitě úkol, na nějž se často v aplikacích theorie grup naráží (na př. v aplikacích na theorii 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 t. zv. normální podgrupy. Abychom mohli alespoň naznačit tyto problémy a jejich řešení, musíme se seznámit s několika dalšími základními, již abstraktními pojmy theorie grup.

Cvičení k 1,5.

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 representována grupou matic

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

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, t. zv. monomiální grupu stupně n. Tato grupa je isomorfní s grupou speciálních t. zv. monomiálních (česky: jednočlenných) (lineárních homogenních) transformací tvaru

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

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

5. Přesvědčte se, že jestliže koeficienty $k_1, k_2, \ldots, k_n$ probíhají pouze čísla z jisté podgrupy násobící 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

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

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

$$\pm \mathfrak{i} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad \pm \mathfrak{j} = \begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix}, \quad \pm \mathfrak{k} = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix},$$

$$\mathfrak{l} = \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}: \text{ pak je}$$

$$\mathfrak{i}^2 = \mathfrak{i}, \quad \mathfrak{j}^2 = \mathfrak{k}^2 = \mathfrak{l}^2 = -\mathfrak{i}, \quad \mathfrak{j}\mathfrak{k} = \mathfrak{l}, \quad \mathfrak{k}\mathfrak{j} = -\mathfrak{l}, \quad \mathfrak{k}\mathfrak{l} = \mathfrak{j}, \quad \mathfrak{l}\mathfrak{k} = -\mathfrak{j},$$
$$\mathfrak{l}\mathfrak{j} = \mathfrak{k}, \quad \mathfrak{j}\mathfrak{l} = -\mathfrak{k}.$$

Sestrojte tabulku: $+\mathfrak{i}$, $+\mathfrak{j}$, $+\mathfrak{k}$, $+\mathfrak{l}$ jsou t. zv. základní Hamiltonovy kvaterniony.

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

9.*Ukažte, že všechny regulární lomené transformace $T(a_1, b_1, a_2, b_2)$ jedné reálné (po př. 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, t. j. 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 t. zv. projektivní grupy).

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

Ukažte, že t. zv. afinní transformace tvaru $x' = a_1 x + b_1$ tvoří podgrupu (zvl. případ t. zv. afinní grupy).

1,6. ROZDĚLENÍ PRVKŮ GRUPY DO TŘÍD DLE PODGRUPY. HOMOMORFNÍ ZOBRAZENÍ, NORMÁLNÍ PODGRUPA, PODÍLOVÁ 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 $x_1 H$ a $x_2 H$ 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. Tedy je 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, t. j. 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 (t. j. 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 t. zv. *cyklické podgrupy*. Je-li G daná grupa a a její prvek, pak cyklická podgrupa je tvořena všemi mocninami prvku a

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

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 t. zv. *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

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

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 t. zv. nekonečnou cyklickou grupu. Nekonečné cyklické grupy jsou zřejmě isomorfní se sečítací 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 t. zv. malá Fermatova[24] věta číselné theorie.

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

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) — 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 t. zv. modulu ($0 = 0 \,.\, n$ je rovněž násobek čísla n). φ je t. zv. *Eulerova*[25] funkce číselné theorie.

Odvození malé Fermatovy věty z našeho důsledku věty 5 bude ukázkou aplikace abstraktní poučky z theorie 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 prvky naší grupy, a za druhé určit pro ně grupové násobení.

Prvky naší grupy budou nikoli snad jednotlivá čísla, nýbrž jisté celé t. zv. zbytkové třídy dle dělitele, t. zv. modulu n, t. j. 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 o rozdílu $b - a = -(a - b)$. (Na př. pro $n = 12$ patří $5^4 = 625 = 52 \,.\, 12 + 1$ do téže zbytkové třídy modulo 12

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

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 $\bar{a}$, takže $\bar{a}=\bar{b}$ 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 theorii 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 $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$.

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 $n=12$ na př. $\varphi(12)=4$. 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 $\bar{0}$, t. j. třída všech násobků modulu n do naší grupy nepatří zatím co třída $\bar{1}$ 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

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

Na př. 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, t. zv. násobící grupě modulo n.

Axiom (1) neomezenosti a jednoznačnosti bude splněn, jestliže předně — kvůli jednoznačnosti — výsledek násobení $\overline{ab}$ třídy $\overline{a}$ třídou $\overline{b}$ 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 $\overline{a}$ a b' do třídy $\overline{b}$, 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 s 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). Neboť nechť $i = q \,.\, n + 1$ je číslo z třídy $\bar{1}$ (t. j. $\bar{1} = \bar{i}$). Nechť libovolné celé číslo x je ze třídy $\bar{x} = \bar{r}$ 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

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

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

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

(Na př. 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

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

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, t. j. utvořme čísla

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

(Na př. 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 $a, aa_1, \ldots, aa_{\varphi(n)}$ 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 $\bar{x} \,.\, \bar{a} = \bar{a} \,.\, \bar{x} = \bar{1}$. (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 $\bar{a}^{-1} = \bar{7} = \bar{a}$.)

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, t. j. 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

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

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 $\bar{a}^{\varphi(n)} = \bar{a}^{mq} = (\bar{a}^m)^q = \bar{1}^q = \bar{1}$ čili opravdu

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

Poznamenejme ještě, že násobící grupy tříd celých čísel nesoudělných s modulem n, jichž jsme právě užili ke grupově theoretickému 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 t. zv. Fermatovu větu theorie grup, to jest tvrzení, že *v grupě řádu N je N-tá mocnina libovolného prvku rovna jednotce grupy, t. j.* $a^N = j$, 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 $a^r, {}^{2r}, {}^{3r}, \ldots, a^{sr} = j$, 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 vytváří v G netriviální cyklickou podgrupu, takže možnost 2 dle předpokladu odpadá. Obráceně 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 t. zv. Fermatovy věty theorie 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 t. zv. 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 modulem, který je sice z jiného materiálu (a po př. menších rozměrů), ale jehož tvar je přesně shodný s tvarem originálu.

Pro mnohé účely však stačí zmíněnou součást stroje kolmo *promítnout* (pomocí deskriptivní geometrie) 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 theorii 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 $\mathfrak{S}_n$ 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**. Na př. 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 permutace π stupně n, jakožto prvku symetrické grupy $\mathfrak{S}_n$, 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 $\mathfrak{S}_n$ na (násobící) grupu čísel $+1$ a -1, což patrně je 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 $(n-1) + (n-2) + \ldots + 1 = \frac{(n-1) \cdot n}{2}$ 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 $\mathfrak{S}_n$ na grupu $(+1, -1)$. Protože zřejmě existují jak permutace sudé, tak i liché každého stupně n, 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 $1, 2, \ldots, n$, 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 $1, 2, \ldots, n$. 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 rovnost $\varepsilon(\varrho\pi) = \varepsilon(\varrho)\,\varepsilon(\pi)$ čili zobrazení ε je vskutku homomorfním zobrazením.

Je jasné, že zde homomorfní obraz, t. j. cyklická grupa řádu 2, je hrubý a vystihuje symetrickou grupu permutací velmi málo.[26]

2. V druhém příkladě bude homomorfní obraz věrnější.

Budiž K (ze školy v podstatě známá) násobící 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 $i = \sqrt{-1}$).

Zobrazme grupu K do násobící grupy R všech reálných čísel kladných tím, že přiřadíme komplexnímu číslu $x + iy$ jeho t. zv. 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

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

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

(jestliže věc nezná ze školy).

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, t. zv. originálu, z grupy G.

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

$$f(x_1x_2) = f(x_1) \cdot f(x_2)$$

(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 k ničemu, 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 $f(j_G) = f(j_G j_G) = f(j_G) \cdot f(j_G)$, 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 representace dané grupy grupou permutací anebo grupou matic. Je to přirozené a důležité rozšíření pojmu isomorfní representace, s nímž jsme se již seznámili. Je zajímavé, že homomorfní representace 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", t. j. homomorfních representací (podobně jako si těleso zrekonstruujeme z jeho nárysu a půdorysu), jestliže známe t. zv. úplný systém homomorfních representací[27] dané grupy, z něhož lze sestrojit isomorfní obraz dané grupy. Vedlo by nás příliš daleko, kdybychom měli podat příklady na to; čtenář, který se odhodlá k hlubšímu studiu theorie grup je nalezne v obšírnějších učebnicích theorie grup.

Obrátíme se k dalšímu důležitému pojmu abstraktní theorie 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 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 $\mathfrak{S}_n$ (všech permutací stupně n) rozpadá homomorfním zobrazením $f = \varepsilon$ (na cyklickou násobící grupu z čísel ± 1) ve dvě třídy, třídu sudých a třídu lichých permutací. V druhém předchozím příkladě se násobící grupa všech od nuly růz-

[27] Úplným nazýváme takový systém homomorfních representací, v němž každý nikoli jednotkový originál obdrží alespoň jednou nikoli jednotkový obraz.

ných 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 $f(x_1 x_2) = f(x_1) \cdot f(x_2) = j_H \cdot j_H = j_H$, 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 přesvědčíme, 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 na příklad 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

$$f(xu) = f(x) \cdot f(u) = f(x) \cdot j_H = f(x),$$

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}, t. zv. konjugovaný prvek k prvku x pomocí (libovolného) prvku z z grupy G.

Tak na př. ze dvou nám známých podgrup grupy euklidovských pohybů roviny (př. 2 v odst. 1,4) 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 $\mathfrak{S}_n$ tvoří t. zv. alternující grupu $\mathfrak{A}_n$ stupně n, která je normální podgrupou v grupě $\mathfrak{S}_n$. — V každé Abelově (komutativní) grupě je ovšem zřejmě každá podgrupa normální. (Obrácené tvrzení neplatí, viz cvič. 7 z odst. 1,5)*.

Důležitost normálních podgrup v grupě vyplývá z toho, že pomocí nich lze z dané grupy tvořit potřebné nové grupy, je-

*) V grupě základních kvaternionů ze cvič. 7 z odst. 1,5 je každá podgrupa normální podgrupou, ačkoli grupa není Abelova.

jímiž 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 $x' = xu_1$ 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 (t. j 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: Podílová grupa grupy G dle normální podgrupy N a značíme $\frac{G}{N}$; 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 podílové grupy $\frac{G}{N}$.

Jaký je zobrazovací vztah podílové grupy $\frac{G}{N}$ k původní grupě?

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

Vraťme se nyní k případu, že normální podgrupa N grupy G je souhrnem originálů jednotky v jakémsi homomorfním zobrazení f grupy G na grupu H. Jaký bude vztah podílové grupy $\frac{G}{N}$ ke grupě H?

Snadno nahlédneme, že tyto grupy jsou si 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 podílové grupy $\frac{G}{N}$ na grupu H je zřejmě homomorfní a kromě toho vzájemně jednoznačné. Shrňme si tedy výsledek předchozích úvah do následující t. zv. první věty o isomorfismu theorie 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 samy t. zv. podílovou grupu $\frac{G}{N}$ při násobení $xN \,.\, yN = xyN$. Podílová grupa $\frac{G}{N}$ 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 podílová grupa $\frac{G}{N}$ je isomorfně zobrazena na grupu H zobrazením $\bar{f}$, daným rovností

$$\bar{f}(xN) = f(x).$$

Uvedená 1. věta o isomorfismu theorie 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:

Podílová grupa $\frac{\mathfrak{S}_n}{\mathfrak{A}_n}$ symetrické grupy stupně n podle její normální alternující podgrupy $\mathfrak{A}_n$ je isomorfní s kteroukoli cyklickou grupou řádu 2, na př. s podgrupou $(+1, -1)$ násobící grupy všech zlomků.

Násobící grupa kladných reálných čísel je isomorfní s podílovou grupou násobící grupy všech komplexních čísel o absolutní hodnotě 1.

Uveďme ještě jeden důležitý příklad na tvoření podílové grupy. Za grupu G vezměme sečítací 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, t. j. jež dávají při dělení modulem n týž nezáporný nejmenší zbytek. Podílová grupa $\frac{G}{N}$ je t. zv. sečítací grupa modulo n.

(Pozor, něco jiného byla t. zv. násobící grupa modulo n, která se skládala jen ze zbytkových tříd, naplněných vesměs čísly, nesoudělnými s modulem, kdežto sečítací grupa modulo n obsahuje všechny zbytkové třídy.) Je-li H jakákoli cyklická

grupa řádu n, na př. násobící grupa všech n n-tých odmocnin z 1, pak první věta o isomorfii nám zde říká, že sečítací grupa modulo n je isomorfní s touto cyklickou grupou.

Tvořením podílové 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 (s 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" (t. j. 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 t. zv. druhou větu o isomorfismu theorie grup. Je to pomocná věta významu theoretického, jejíž užití si ukážeme v par. 1,6.

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 podgrupa v grupě G.* (Takový souhrn UN je t. zv. spojení podgrup U a N.)

2. *Souhrn označený jako $U \cap N$ všech prvků z grupy 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 podílové grupy $\frac{UN}{N}$ *a* $\frac{U}{U \cap N}$ *jsou navzájem isomorfní.*

Důkaz:

Nejprve k bodu 1:

Máme ukázat především, že součin dvou násobků tvaru $u_1 n_1$ a $u_2 n_2$, 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

$$(u_1 n_1)(u_2 n_2) = u_1 u_2 (u_2^{-1} n_1 (u_2^{-1})^{-1} n_2).$$

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 $u = u_1 u_2$ pak leží v U, protože U je podgrupa obsahující u_1 i u_2. Z rovností $(u_1 n_1)^{-1} = n_1^{-1} u_1^{-1} = u_1^{-1} (u_1 n_1^{-1} u_1^{-1})$ je pak již snadno patrno, že UN je vskutku podgrupou v A.

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 podílová grupa $\frac{UN}{N}$ tvoří

zřejmě podgrupu podílové grupy $\frac{G}{N}$, protože obsahuje ty levé třídy dle N, které mají nějaký prvek v podgrupě U. Při námi známém homomorfním zobrazení $x \to xN$ celé grupy G na podílovou grupu $\frac{G}{N}$ zobrazíme tedy patrně podgrupu U (grupy G) tímto homomorfním zobrazením na podílovou podgrupu $\frac{UN}{N}$. Nyní užijeme hlavní části 1. věty o isomorfismu. V podgrupě U tvoří originály jednotky normální podgrupu N' tak, že podílové grupy $\frac{U}{N'}$ a $\frac{UN}{N}$ jsou navzájem isomorfní. Jednotkovým prvkem v podílové grupě $\frac{UN}{N}$ 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 dalšímu paragrafu, zaveďme si ještě jeden základní pojem theorie grup: pojem jednoduché grupy.

Tak jako (vzhledem k dělitelnosti) hledíme celá (složená) čísla vystihovat čísly jednoduchými, t. j. 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 par. 1,7.

Za jednoduchou budeme jistě považovat na př. 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 podílové 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. po 1,7) a při konečných grupách není jednoduchost grupy nikterak spojena s jednoduchostí jejího řádu (jak dále uvidíme).

Zvláštní a pro theorii rovnic důležitý druh konečných jednoduchých grup tvoří alternující grupy permutací stupně aspoň pátého. Těm se budeme věnovat v příštím paragrafu, čímž skončíme systematickou část výkladu základních pojmů theorie grup.

Mnohý z čtenářů bude snad ke své malé radosti konstatovat, že úvahy dalšího paragrafu jsou obtížnější, než to, co předcházelo. Je to pochopitelné: prozatím jsme se omezovali na nejzákladnější pojmy theorie grup a jejich vzájemné nejjednodušší souvislosti. V podstatě jsme tím jen třídili bohatý materiál zjevů, ovládaných grupovou zákonitostí, aniž jsme se o mnoho povznesli nad zevšeobecňování poznatků známých v matematice i bez theorie grup. Úsudky byly sice mnohde dosti abstraktní, zato však velmi prosté a průhledné. Tam, kde theorie grup skýtá hlubší a podstatně nové výsledky, jež (jako na př. v následujícím) vedly k novým

matematickým objevům, tam je již třeba vyvinout značně větší myšlenkové úsilí, abychom dobře pochopili základní myšlenku důkazu a její realisaci. Pokusím se čtenáři toto pochopení co nejvíce usnadnit, t. j. provést důkaz do podrobností, při tom ale nenechat v těchto podrobnostech zaniknout hlavní motiv celé úvahy, jehož rozvíjením a ověřováním právě důkaz je.

Cvičení k 1,6.

1. Jaké jsou podgrupy v grupě $\mathfrak{S}_3$ (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 sečítací grupě celých čísel. Totéž pro násobky čísel 2, 4, 5. Jaké jsou vůbec všechny podgrupy sečítací grupy celých čísel?

3. Ukažte, že v symetrické grupě $\mathfrak{S}_n$ (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 $\mathfrak{S}_{n-r}$. 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 $\mathfrak{S}_3$ 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 násobící grupy všech reálných čísel $\neq 0$ na násobící grupu všech kladných čísel reálných.

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

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 násobící 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

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

($a \neq 0$, t. zv. 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, že podílová 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 podílové grupy, vyhledejte k libovolné tam ležící matici

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

matici

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

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 t. zv. grupu representantů tříd, která je isomorfní s uvedenou podílovou grupou.)

11. Co je dle 1. věty o isomorfii normální podgrupou originálů jednotky při homomorfním zobrazení $f(n) = i^n$ ($i = \sqrt[+]{-1}$) sečítací grupy celých čísel na násobící 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, pak je podílová grupa $\frac{HN}{N}$ isomorfní s podgrupou H. Jestliže ještě každý prvek grupy G se dá psát jako součin prvku z H s prvkem z N, pak podílová grupa $\frac{G}{N}$ je isomorfní s podgrupou H. (Jako ve cvič. 10 je H pak grupou representantů k podílové grupě $\frac{G}{N}$.) — Dokažte.

13.* Budiž G sečítací 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.

1,7. TŘÍDA KONJUGOVANÝCH PRVKŮ. NORMALISÁTOR PRVKU. TŘÍDOVÁ ROVNICE. KONJUGOVANÉ PERMUTACE. JEDNODUCHOST ALTERNUJÍCÍ GRUPY $\mathfrak{A}_n$ 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 $a = xax^{-1}$, t. j. $ax = xa$. (Říkáme, že x je prvek komutativní s prvkem a.) Mezi takové prvky patří předně jednotka j naší grupy G. Jestliže $a = x_1 a x_1^{-1}$, $a = x_2 a x_2^{-1}$, pak dosazením máme

$$a = x_1 x_2 a x_2^{-1} x_1^{-1} = x_1 x_2 a (x_1 x_2)^{-1},$$

takže se dvěma prvky x_1 a x_2 i jejich součin $x_1 x_2$ 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*, t. zv. normalisátor 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 t. zv. 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 $\varrho\pi\varrho^{-1}(k)$, t. j. 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, t. j.

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

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

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

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

Avšak permutace, konjugované k dané permutaci a jejich počet lze ještě lépe přehlédnout pomocí t. zv. 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, ..., ... n) *se dá jednoznačně rozložit v součin oddělených cyklů, při čemž na pořadí činitelů nezáleží.*

Budiž tedy π jakákoli neidentická permutace, provedená na číslech 1, 2, ..., n. Najděme si první číslo i_1, které nezůstává stát při permutaci π, $\pi(i_1) \neq i_1$. Pak se mezi čísly $\pi(i_1)$, $\pi^2(i_1)$, $\pi^3(i_1)$, ..., $\pi^t(i_1)$; ... 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 $\pi^r(\pi^s)^{-1} = \pi^{r-s}(i_1) = i_1$.

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 $\pi^k(i_1) = i_1$ (po prvé). 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 permutací π se 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 $m_2 = \pi(m_1), m_3 = \pi^2(m_1), \ldots, m_q = \pi^{q-1}(m_1)$, kdežto $\pi^q(m_1) = m_1$ (po prvé). 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, t. j. 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 (t. j. 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 na př., 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 $(i_1 i_2 \dots i_k)$ je daný cyklus, pak patrně permutace jím dosažená je rovna sledu postupně provedených výměn (transposic) tak, že možno psát

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

(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 žádném 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. 1,5).

A nyní se obraťme k alternující grupě $\mathfrak{A}_5$ všech sudých permutací stupně 5.

Věta 10.

Alternující grupa $\mathfrak{A}_5$ (*sudých permutací z pěti předmětů*) *je jednoduchá.*

Důkaz povedeme methodou, o níž již byla zmínka: určíme počet permutací ve třídách vzájemně konjugovaných permu-

tací, na něž se rozpadá grupa $\mathfrak{A}_5$, a ukážeme prostě, že z čísla 1 a některých sčítanců, udávajících počet konjugovaných permutací v $\mathfrak{A}_5$, nelze obdržet součet, který by dělil řád grupy $\mathfrak{A}_5$, t. j. číslo, jež by mohlo být řádem normální podgrupy. Při tom musíme dát pozor na to, že půjde o konjugovanost v $\mathfrak{A}_5$ (a nikoli v $\mathfrak{S}_5$), t. j. o konjugovanost pomocí sudých permutací.

Podle rozkladu v oddělené cykly nalézáme tyto druhy sudých permutací stupně 5 — jichž je $\frac{1}{2}5! = $ řád $\mathfrak{A}_5 = 60$ (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 $\mathfrak{A}_5$. Jejich počet obdržíme, kombinujíce každou z $\binom{5}{2}$[28] dvojic čísel s $\binom{3}{2}$ zbývajícími dvojicemi a dělíce dvěma, protože takto obdržíme každý součin dvou oddělených transposic dvakrát.

[28] $\binom{n}{k}$ je ze školy známý binomický koeficient,

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{1\,.\,2\,.\,3\dots k}.$$

Tedy první třída vzájemně konjugovaných permutací v grupě $\mathfrak{A}_5$ 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 $2 \cdot \binom{5}{3} = 20$ trojčlenných cyklů v $\mathfrak{A}_5$. 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 $\mathfrak{A}_5$ 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 $\mathfrak{A}_5$.) Je vidět, že jedinými permutacemi, pomocí nichž pětičlenný cykl je konjugován sám se sebou, je tento cykl sám a jeho mocniny. Jinými slovy, normalisátor pětičlenného cyklu v $\mathfrak{A}_5$ je tvořen právě všemi pěti různými mocninami tohoto cyklu. Ještě jinak řečeno, třída všech v grupě $\mathfrak{A}_5$ konjugovaných permutací k pětičlennému cyklu obsahuje

$$\frac{\text{řád } \mathfrak{A}_5}{5} = \frac{60}{5} = 12 \text{ permutací.}$$

Rozpadá se tedy všech 24 pětičlenných cyklů v $\mathfrak{A}_5$ do dvou takových tříd vzájemně konjugovaných, obě po 12 permutacích (prvcích grupy $\mathfrak{A}_5$).

Třídová rovnice pro alternujícígrupu $\mathfrak{A}_5$ tedy zní

$$\tfrac{1}{2}5! = 60 = 1 + 15 + 20 + 12 + 12.$$

Jako řády (netriviální) normální podgrupy v $\mathfrak{A}_5$ 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, t. j. čísla 60. — Tedy skutečně alternující grupa $\mathfrak{A}_5$ nemůže mít netriviálních normálních podgrup.

Ukazuje se, že všechny další alternující grupy jsou jednoduché. Myšlenku důkazu tohoto na první pohled překvapujícího zjevu 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 $\mathfrak{A}_n$ (která je ovšem podgrupou následující alternující grupy $\mathfrak{A}_{n+1}$) vyplývá (užitím 2. věty o isomorfismu), že naopak netriviální normální podgrupa v $\mathfrak{A}_{n+1}$ musí obsahovat „velmi málo" permutací; z tohoto rozporu vyplývá, že nemá-li $\mathfrak{A}_n$ netriviálních normálních podgrup, nemá je ani $\mathfrak{A}_{n+1}$. Protože však alternující grupa $\mathfrak{A}_5$, jak již víme, jednoduchá je, je jednoduchá i následující alternující grupa $\mathfrak{A}_6$, následkem toho je jednoduchá i další alternující grupa $\mathfrak{A}_7$, atd. až do nekonečna.

Náš postup důkazu jednoduchosti alternujících grup stupně vyššího než pátého, který následuje, je tedy t. zv. *induktivním* postupem. (O různých druzích a povaze takových úsudků t. zv. matematickou indukcí se čtenář poučí ve svazečku „Cesty" od Katětova, pod názvem „Jaká je logická výstavba matematiky".)

Věta 11.

Alternující grupa $\mathfrak{A}_n$ stupně n většího než čtyři je jednoduchá.

Důkaz:

Alternující grupa $\mathfrak{A}_5$ je jednoduchá podle předchozí věty. Kdyby některá z dalších alternujících grup $\mathfrak{A}_n$ pro $n > 5$ nebyla jednoduchá, musela by mezi nimi být jedna alternující

grupa, řekněme $\mathfrak{A}_m$, co nejmenšího stupně m (ovšem že je $m > 5$) taková, že ona sama již jednoduchá není, ale předchozí alternující grupa $\mathfrak{A}_{m-1}$ ještě jednoduchá je. Ukážeme, že existence takové první nikoli jednoduché alternující grupy $\mathfrak{A}_m$ je vyloučena, protože by vedla k odporujícím si důsledkům. (T. zv. důkaz nepřímý, srov. citovanou Katětovovu knížku.)

Předpokládejme tedy, že máme v alternující grupě $\mathfrak{A}_m$ ($m > 5$) netriviální normální podgrupu $\mathfrak{N}$ (která tedy obsahuje více než jenom identickou permutaci).

Prvním naším (pomocným) krokem bude nalézt v $\mathfrak{N}$ 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 $\mathfrak{N}$ 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 disposici) zjišťujeme v naší normální podgrupě $\mathfrak{N}$ přítomnost permutace

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

a tedy i 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 $\mathfrak{N}$ 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 $\mathfrak{N}$, 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 $\mathfrak{A}_m$), 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'.[29] Takovou sudou permutaci π si snadno sestrojíme prostě tak, že ještě určíme zcela libovolně v co mají přejít zbývající čísla — to jsou 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 $\mathfrak{N}$, 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 $\mathfrak{N}$ 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 $\mathfrak{N}$ obsahovat dalších $m - 3$ permutací, převádějících číslo 1 v číslo 3 a současně číslo m ve zbývající čísla. Podobně vždy dalších

[29] 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.

$m - 3$ permutací v $\mathfrak{N}$ je zaručeno při přechodu čísla 1 v čísla 4, 5, ..., m. Celkem tedy obsahuje naše normální podgrupa $\mathfrak{N}$ nejméně $(m - 3)(m - 1)$ různých permutací; řád grupy $\mathfrak{N}$ musí dosáhnout anebo překročit číslo

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

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

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

$$\frac{\mathfrak{A}_{m-1}}{\mathfrak{A}_{m-1} \cap \mathfrak{N}} \cong \frac{\mathfrak{A}_{m-1}\mathfrak{N}}{\mathfrak{N}},$$

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

Předmět, t. j. číslo, které mají nechat stát permutace z $\mathfrak{A}_{m-1}$, si nyní zvolíme tak, aby podgrupa $\mathfrak{N}$, (která byla předpokládána jako netriviální, t. j. různá od celé grupy $\mathfrak{A}_m$), neobsahovala podgrupu $\mathfrak{A}_{m-1}$, čili aby průnik $\mathfrak{A}_{m-1} \cap \mathfrak{N}$ nebyl roven $\mathfrak{A}_{m-1}$. Že to vždy lze (za našich předpokladů), to poznáme takto: V opačném případě by $\mathfrak{N}$ musela obsahovat každou z možných podgrup $\mathfrak{A}_{m-1}$ (pro různě zvolená při permutacích stálá čísla), t. j. $\mathfrak{N}$ by obsahovala veškeré sudé permutace (na našich m předmětech, resp. číslech), které nechávají stát aspoň jedno číslo. Jakožto podgrupa obsahovala by $\mathfrak{N}$ veškeré součiny takových permutací. Avšak tím by již $\mathfrak{N}$ obsahovala všechny sudé permutace (stupně m) vůbec. Neboť rozložme každou z dalších sudých permutací (t. j. 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 $\mathfrak{A}_{m-1}$ v $\mathfrak{A}_m$ tak, aby nebyla obsažena v normální podgrupě $\mathfrak{N}$, máme v průniku $\mathfrak{A}_{m-1} \cap \mathfrak{N}$ normální podgrupu (pod)grupy $\mathfrak{A}_{m-1}$, která je od $\mathfrak{A}_{m-1}$ různá. Avšak $\mathfrak{A}_{m-1}$ je podle předpokladu ještě jednoduchá grupa, tedy nezbývá než že $\mathfrak{A}_{m-1} \cap \mathfrak{N}$ se redukuje na pouhou jednotku (identickou permutaci).

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

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

z čehož plyne, že řád naší normální podgrupy $\mathfrak{N}$ grupy $\mathfrak{A}_m$ je nanejvýše roven číslu m.

Avšak prve jsme dokázali, že řád grupy $\mathfrak{N}$ musí být větší anebo nejvýše roven číslu $m^2 - 4m + 3$. Z toho ovšem vyplývá, že $m^2 - 4m + 3 \leqq m$, t. j. 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 $\mathfrak{A}_m$ 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 $\mathfrak{A}_n$ všech stupňů n, vyšších, než 4 bylo důležitým krokem v počátcích samotné theorie 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 theorii grup, v t. zv. Galoisově[30] theorii algebraických rovnic tvaru

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

t. j. t. zv. 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 theorie. Musíme se spokojit s pouhým poukazem na to, že Galoisova theorie převádí vlastnosti algebraické rovnice o jedné neznámé ve vlastnosti jisté t. zv. Galoisovy grupy permutací kořenů této rovnice. Vlastnostem grupy odpovídají vlastnosti rovnice a naopak. Zejména řešitelnosti rovnice pomocí t. zv. 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 však 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 je tomu u rovnic druhého (to čtenář zná), třetího a čtvrtého stupně (to čtenář možná nezná, ale takové

[30] Pěkný výklad Galoisovy theorie nalezne čtenář na př. v polské učebnici vyšší algebry: Šierpiński, *Zarys algebry wyszej* (Monografie matematyczne Warszawa 1948) jako dodatek od prof Mostowského.

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 konkretních 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 stupně a vyššího, které trvalo dobrá tři staletí.

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

Cvičení k 1,7.

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 $(1\,3\,5)^2 = (1\,5\,3)$). *Jaké pravidlo mocnění cyklů lze vyslovit pro to, kdy se cykl mocněním rozpadá?

2. Najděte konjugované permutace

$$\varrho\pi^3\varrho^{-1},\ \sigma\varrho\sigma^{-1},\ \varrho\sigma\varrho^{-1},\ \pi^3\varrho\pi^{-2}$$

k permutacím π^3, ϱ, σ ze cvič. 1,2.)

3. Proveďte rozdělení permutací do tříd konjugovaných pro grupy $\mathfrak{S}_3$ a $\mathfrak{S}_4$ podrobně. Napište třídové rovnice.

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

5. Nazveme sudou permutací 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. (Zatím co $\pi'(k) = \pi(k)$ pro $k = 1, 2, ..., n$.) 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 $\mathfrak{A}$ při definici násobení

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

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

6.*Dokažte, že nekonečná grupa $\mathfrak{A}$ neobsahuje vlastní normální podgrupu čili že je příkladem nekonečné jednoduché grupy. (Návod: Kdyby $\mathfrak{N}$ byla normální podgrupa v $\mathfrak{A}$, pak průnik $\mathfrak{A}'_n \cap \mathfrak{A}$ by byla normální podgrupa v podgrupě $\mathfrak{A}'_n$ (jak víme z 2.věty o isomorfii). Následkem jednoduchosti podgrup $\mathfrak{A}'_n$ pro $n = 5, 6, 7, \ldots$ (dle cvič. 6) musí buďto: $\mathfrak{A}'_n \cap \mathfrak{N} = \mathfrak{A}'_n$ čili $\mathfrak{A}'_n$ je podgrupou i v normální podgrupě $\mathfrak{N}$, anebo: $\mathfrak{A}'_n \cap \mathfrak{N}$ obsahuje jen identickou permutaci (jednotku). Nastává-li druhá možnost pro všechna $n = 5, 6, 7$ pak snadno ukážete, že $\mathfrak{N}$ obsahuje jen jednotku. V opačném případě $\mathfrak{A}'_m \cap \mathfrak{N} = \mathfrak{A}'_m$ pro jisté $m > 5$ zase snadno ukážete, že $\mathfrak{N}$ obsahuje každou podgrupu $\mathfrak{A}'_r$ pro $r > m$ a tedy že $\mathfrak{N}$ je rovna celé grupě $\mathfrak{A}$.)

7. Dokažte jednoduchost všech alternujících grup $\mathfrak{A}_n$ pro $n \neq 4$.

1,8. KOMPOSIČNÍ ŘADY. DIREKTNÍ ROZKLADY. p-GRUPY A SYLOWOVY PODGRUPY. GRUPY A TOPOLOGIE. ZÁVĚR.

Jedním z hlavních úkolů theorie grup, jak již bylo poznamenáno, je probádat, jak jsou grupy budovány ze svých podgrup. Jsou dva hlavní způsoby, kterými sledujeme jak pod-

grupy skládají grupu: t. zv. komposiční řada a t. zv. 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 $G_1, G_2, G_3, \ldots, G$ e tvoří t. zv. komposiční řadu grupy G. Počtu n podgrup v komposiční řadě vystupujících se říká délka komposiční řady. Podílovým grupám $\frac{G_i}{G_{i+1}}$ říkáme někdy faktory komposiční řady. Je důležité si povšimnout, že podmínku 3 lze právě tak dobře nahradit podmínkou

3'. Faktory komposiční řady, t. j. podílové grupy $\frac{G_i}{G_{i+1}}$, jsou jednoduché grupy. (Neboť každá normální podgrupa G' grupy G_i, obsahující grupu G_{i+1} dává vznik normální podgrupě $\frac{G'}{G_{i+1}}$ podílové grupy $\frac{G_i}{G_{i+1}}$ a obráceně).

Uveďme si alespoň dva příklady komposiční řady:

1. Symetrická grupa $\mathfrak{S}_n$ pro $n \geqq 5$ má komposiční řadu $\mathfrak{S}_n$, $\mathfrak{A}_n$, (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 $\mathfrak{A}_n$ v $\mathfrak{S}_n$ je tam totiž normální podgrupou, neboť se sudou permutací ϱ je i každá s touto konjugovaná permutace $\pi\varrho\pi^{-1}$ sudá — a podílová grupa $\frac{\mathfrak{S}_n}{\mathfrak{A}_n}$ je, jak víme, cyklická grupa řádu 2, tedy grupa jednoduchá; alternující grupa $\mathfrak{A}_n$ je pak sama již, jak víme z předchozího par., jednoduchá grupa.

2. Cyklická grupa řádu 12, skládající se z mocnin

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

má komposiční řadu složenu ze 4 následujících cyklických podgrup; celá grupa (a) sama (tvořena všemi mocninami prvku a), podgrupa (a^3) vytvořená 4-mi různými mocninami $a^3, a^6, a^9, a^{12} = j$ 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 komposiční řada. Jiná komposiční řada se skládá z podgrup (a), (a^2) (a^6), (j) — při stejném vyznačování cyklických grup. (O normálnost podgrupy v předchozí podgrupě komposiční řady se zde netřeba starat — vzhledem ke komutativitě dané grupy.)

O komposičních řadách platí nyní pozoruhodná věta Jordan-Höldero va, která dalekosáhle odhaluje strukturní uložení podgrup v grupě:

Délka dvou různých komposičních řad téže grupy je táž. Co více, ke každému faktoru jedné komposiční řady existuje s ním isomorfní faktor druhé komposiční řady, takže faktory obou komposičních řad jsou až na isomorfismus a pořadí tytéž.[31]

(Povšimneme si, že Jordan-Hölderova věta sama nás nepoučuje o tom, zda daná grupa vůbec komposiční řadu má, ona jen vypovídá o vlastnostech komposičních řad v případě, že nějaké máme. Existence komposičních řad je zřejma v případě konečných grup. V zobecnění na 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 pořadového čísla, viz Pospíšilovo „Nekonečno v matematice" ve sbírce „Cesta k vědění") věta Jordan-Hölderova platí, pro stoupající nikoli. Jordan-Hölderova věta má rovněž značný význam ve zmíněné již Galoisově theorii 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 t. zv. 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 $p_1, p_2, \ldots, \ldots, p_r$, tedy

[31] Francouz C. Jordan objevil rovnost délek komposičních řad téže grupy. Němec O. Hölder později objevil tvrzení o „rovnosti" (t. j. isomorfismu) faktorů. Dalekosáhlé zobecnění na komposiční řady „nekonečné" délky podal nedávno sovětský matematik A. Kuroš. Dalším vyšetřováním platnosti zobecněné Jordan-Hölderovy věty (ve svazech) se zabývá v přítomné době u nás prof. Vl. Kořínek.

$$a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

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 násobící grupy kladných zlomků. Při tom všechny mocniny jednoho a téhož prvočísla p s kladnými i zápornými mocniteli $\dots, p^{-2}, p^{-1}, p^0 = j, p^1, p^2, \dots$ tvoří zřejmě normální (nekonečnou cyklickou) podgrupu v násobící grupě všech kladných zlomků. Každé kladné lomené 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 (lomených 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, t. j. k pojmu direktního rozkladu grupy v direktně nerozložitelné podgrupy:

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

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

$$G = G_1 \times G_2 \times \dots$$

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 násobící grupy kladných zlomků 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 násobící grupy *všech* zlomků, t. j. 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: sečítací grupa komplexních čísel $x + i \,.\, y$ ($i = \sqrt{-1}$). (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 sečítací grupy reálných čísel, tvořené jednak t. zv. reálnými částmi x, jednak t. zv. imaginárními částmi y komplexního čísla $x + i \,.\, y$.

Poněkud obecněji je direktním rozkladem ve tři vzájemně rozlišené sečítací grupy reálných čísel dána sečítací grupa všech vektorů v prostoru $x \,.\, i + y \,.\, j + z \,.\, k$ (i, j, k jsou t. zv. 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 násobící grupu všech racionálních čísel tvaru 2^k3^h, tedy čísel $1, 2, \frac{1}{2}, 3, \frac{1}{3}, 4, \frac{1}{4}, 6, \frac{1}{6}, 9, \frac{1}{9}, \ldots$ Za jeden faktor direktního rozkladu grupy G položme podgrupu $G_1 = (2^k)$ $(k = 0, \pm 1, \pm 2, \ldots)$ (t. j. nekonečnou cyklickou grupu vytvořenou všemi celými mocninami čísla 2). Za druhý faktor direktního rozkladu pak zřejmě můžeme vzít podobně (násobící) 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 na př. grupu $G_2' = (6^r)$ $(r = 0, \pm 1, \pm 2, \ldots)$ mocnin čísla 6. Neboť je

$$2^k3^h = 2^{k-h}2^h3^h = 2^{k-h}6^h$$

a rozklad čísla 2^k3^h v součin mocnin čísla 2 a čísla 6 je jednoznačný. (Jestliže totiž je $2^r6^s = 2^{r'}3^{s'}$, 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 direktně nerozložitelné faktory. A přece různé direktní rozklady téže grupy v direktně nerozložitelné faktory jsou v jistém smyslu rovnocenné. O tom nás poučuje základní věta theorie direktního rozkladu grup, t. zv. věta Remak-Schmidtova.[32] Tuto větu, která je protějškem k větě

[32] 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 prof. Kořínek.

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 v obou 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 rokladu 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 násobící grupy G všech čísel tvaru $2^k 3^h$ nám říká m. j. 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 methoda 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 t. zv. p-grupy. Theorie 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 theorie 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 na př. 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 podílová 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 t. zv. Sylowovy podgrupy dané grupy. Jsou to p-grupy s co největším mocnitelem n řádu p^n, které jsou obsaženy v dané konečné grupě. Theorie 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 na př. 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 theorie 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 theorii grup budování složitějších grup z jednodušších podgrup.

Na ukončenou 1. části knížky se obraťme alespoň k nejhrubšímu náčrtu jisté theoreticky důležité aplikace theorie grup, totiž aplikace na t. zv. topologii. Jde o spojení theorie 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[33] je od geometrie odštěpená theorie těch 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 t. zv. topologické transformace (deformace) není jednoduché. Spokojíme se zde s přibližným objasněním tohoto pojmu na názorných příkladech.

Mysleme si geometrický útvar, na př. kruh v rovině z dokonale roztažitelného materiálu, na př. na povrchu gumy.

[33] 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. Brouwerem koncem minulého a začátkem tohoto století, stala se topologie jednou z nejdůležitějších základních theorií moderní matematiky. Z vynikajících současných topologů jmenujme sovětské topology Alexandrova a Pontrjagina, z Američanů Alexandera a Lefschetze. Z našich současných matematiků podstatně přispěl k rozvoji moderní topologie laureát státní ceny z matematiky 1951 prof. Čech, v nedávné době pak doc. Katětov.

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 na př. 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 na př. 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 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 na př. v těleso podoby prstence (t. zv. anuloid). Tedy povrch hliněného hrnce s jedním uchem je na př. 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 uhníst 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 t. zv. kombinatorické methody. Ta je právě oním mostem, který spojuje abstraktní pojem grupy s hlubokým rozborem našich nejzákladnějších geometrických t. zn. topologických pojmů tvaru, rozprostření a (vzájemného) uložení a spojitosti. Pokusme se pochopit základní myšlenku kombinatorické methody 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, na příklad 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 jedinných stanic) a ze „spojů", t. j. 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 spojen se tím neruší. Tak se projeví topologická rozdílnost povrchu našeho prstence od povrchu koule na př. 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 vyhlédneme 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 t. zv. 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 by

chom 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 t. zv. 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 (s 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 t. zv. 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 theorie 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 theorii grup samotnou. Jsou to t. zv. volné grupy; tímto názvem vyznačujeme přesně definovanou a tyto grupy charakterisující vlastnost, která — zběžně řečeno — značí, že prvky takové grupy jsou vzájemně vázány (pomocí grupového násobení) co nejslabšími vztahy, t. j. jen takovými, které již nutně vyplývají ze splnění axiomů grupy.

Volné grupy cest jsou ovšem sotva počátkem kombinatorické topologie. Jsou oním základním schematem, které dovoluje vyjadřovat topologické vlastnosti ploch pomocí jistých rovností mezi prvky grupy cest, anebo lépe (což je ale logicky totéž) pomocí jistých, podílových grup utvořených z grupy cest. Vlastním prostředkem topologie jsou teprve tyto podílové grupy. Nejdůležitější na věci je, že tyto podílové grupy závisejí jen na topologické povaze útvaru (na př. 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 topolo-

gicky charakterisující podílové grupy, jež sestrojujeme v grupě cest pomocí zmíněných rovností. Tyto podílové grupy, t. zv. grupy Bettiho, jsou komutativními grupami, takže pro většinu zásadních úkolů topologie vystačíme s mnohem jednodušší theorií komutativních grup. (O tom se čtenář může poučit ve velmi přístupně psané knížce od znamenitého sovětského topologa Alexandrova, která je prozatím u nás dostupná jen v německém jazyce s názvem *Einfachste Grundbegriffe der Topologie*, vyd. Springer Berlin 1932. Úvod do „nekomutativní" topologie, vycházející z volných grup cest, je v knížce K. Reidemeister, *Einführung in die kombinatorische Topologie*, vyd. Vieweg Braunschweig 1932.)

1,9. ZÁVĚR 1. ČÁSTI KNÍŽKY.

V předchozím, posledním paragrafu 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 theorii grup a jejich užitích nestačili prohlédnout zblízka.

Neuškodí však také přehlédnout jediným krátkým pohledem za sebe tu cestu — tu malou počáteční část výstupu k theorii 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 stej-

ný 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 druhé grupy — a obráceně. Vyzdvihli jsme, že vlastním předmětem bádání abstraktní theorie grup nejsou samotné (konkretní) grupy, nýbrž hned celé typy grup navzájem isomorfních. Tím poučky abstraktní theorie 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 konkretisace a realisace abstraktních pojmů theorie grup. To bylo ukázáno především na isomorfní representaci každé abstraktní konečné grupy, lépe řečeno: každého z možných typů isomorfismu konečných grup, konkretní grupou číselných matic. (Byl předveden ovšem jen nejjednodušší, prakticky i theoreticky málo významný ukázkový způsob takové representace.)

Věnovali jsme se dále několika více méně namátkou vybraným příkladům základních pouček abstraktní theorie grup a příslušných důkazových method. 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 theorie grup.

THEORIE SVAZŮ.

2,1. POVŠECHNÝ ÚVOD.

Nejprve několik slov úvodem k této druhé části knížky.

Výklad některých nejzákladnějších pojmů theorie svazů (a jejich aplikací) je pojat jako předchozí výklad počátků theorie grup, jenom je ještě více omezen úzkým výběrem látky a snad (místy) je *abstraktnější*. Pokud jde o stručnost a *abstraktnost*, odůvodňuji ji předpokladem, že čtenář, který sledoval výklad o grupách, je připraven na takový myšlenkový postup.

Jinak ovšem tato část knížky, pojednávající o *svazech* (svaz — rusky a polsky: *struktura*, angl. a franc.: *lattice*, něm.: *Verband*) je natolik samostatná, že ji lze číst i bez znalosti předchozí části pojednávající o grupách. Nicméně tento postup nedoporučuji, protože se budu častěji odvolávat na analogie a rozdíly mezi svazy a grupami.

Načrtněme si předem pojem svazu v nejhrubších rysech za pomoci takového hrubého porovnání theorie grup s theorií svazů, abychom si učinili předem letmý obraz o neznámé zemi dříve, než do ní vstoupíme.

Na pojmu grupy jsme se seznámili s velmi rozšířeným druhem úkonu, zvaného obecně (grupové) násobení. Tento druh úkonu byl vymezen čtyřmi axiomy theorie grup, které musely být splněny, aby se daný úkon právě mohl nazývat grupovým násobením a aby matematické předměty, na nichž se tento úkon provádí, se mohly jmenovat prvky (elementy) grupy. Název „násobení" pro takový grupový úkon (kterým však může být i běžné sčítání čísel) byl zvolen m. j. proto, že

násobení číselných matic je, jak jsme si ukázali, prototypem obecného grupového násobení.

V posledních asi dvaceti letech byla v matematice seznána podstata a důležitost jisté dvojice na sebe vázaných úkonů povahy méně aritmetické (číselné) a spíše snad geometrické, které je ovládáno poněkud jinou zákonitostí, než je zákonitost, vyjádřená čtyřmi axiomy theorie grup.

Zvláštním a důležitým případem tohoto dvojího úkonu je totiž (geometrické) spojování a protínání prováděné na bodech, přímkách, rovinách a po případě i na jejich vícerozměrných zobecněních.

Užíváme tedy v theorii svazů geometrického názvosloví o spojení a průseku i v abstraktním smyslu, hovoříce o spojování a protínání i tam, kde o bezprostředně geometrické spojování a protínání nejde — podobně jako jsme hovořili o násobení v grupě, jejímiž prvky nikterak nebyla čísla. S takovým dalekosáhle zobecněným spojováním a protínáním, jakožto se dvěma úkony, které jsou spolu nerozlučně spojeny, máme co činit vždy, když jsou splněny (v souhrnu spojových a protínaných předmětů) jisté charakteristické axiomy, t. zv. axiomy theorie svazů, či stručněji svazové axiomy. Tyto axiomy, které si brzy vysvětlíme, jsou zčásti podobné axiomům theorie grup, zčásti jsou však úplně jiného rázu.

Pro souhrn matematických předmětů — opět t. zv. prvků, které lze ve smyslu zmíněných axiomů theorie svazů bez omezení spojovat a protínat, užíváme prostě názvu svaz, podobně jako jsme obecně rozuměli pod slovem grupa souhrn jakýchkoli předmětů, které bylo lze mezi sebou „násobit" ve smyslu axiomů theorie grup.

Základy abstraktně-algebraického pojetí theorie svazů položil německý matematik R. Dedekind na počátku tohoto století. Speciální druh svazů, t. zv. Booleovy algebry, však poznal a studoval již v 1. pol. 19. stol. anglický matematik G. Boole. Dedekindovy práce upadly v zapomenutí až do desítiletí 1930—1940. Od té doby se theorie svazů neobyčejně rozrostla do šířky i do hloubky. Ukázalo se,

že pojem svazu se vyskytuje v mnoha zdánlivě odlehlých odvětvích matematiky a má užití nejen v různých matematických theoriích samotných, nýbrž přímo i v elektrotechnické a statistické praxi. Dá se říci, že úloha theorie svazů v současné matematice je podobná úloze theorie grup (i když je menší; ostatně mezi oběma theoriemi jsou i četné vnitřní souvislosti). To vše jsou důvody, proč jsem považoval za vhodné napsat uvedení do nejzákladnějších pojmů teorie svazů do této knížky, a umístit je právě za část, pojednávající o grupách.

2,2. ČÁSTEČNÉ USPOŘÁDÁNÍ A POLOUSPOŘÁDÁNÍ. POJEM SVAZU NA ZÁKLADĚ POJMU POLOUSPOŘÁDÁNÍ.

Přirozená cesta, kterou jsme zvolili, abychom se dostali k obecnému pojmu grupy, vyšla z pojmu (geometrické) pravidelnosti, tedy z pojmu, jenž je velmi obecný a každému povědomý.

Přirozeným východiskem cesty k obecnému pojmu svazu je pojem snad ještě názornější a každému dobře známý. Je to pojem částečného uspořádání. Zdržíme se poněkud u tohoto pojmu pro jeho značnou (na theorii svazů nezávislou) samostatnou důležitost.

Nejprve, co rozumíme uspořádáním, t. j. úplným uspořádáním nějakého souboru nějakých prvků. (Přívlastek „úplný" se však vynechává a rozumí se sám sebou.)

Čtenáři je dobře známo, že celá, racionální, reálná čísla jsou přirozeným způsobem uspořádána dle velikosti, t. j. o každých dvou takových číslech x a y lze říci, zda je $x < y$ (x menší než y čili na číselné ose leží x před y) anebo zda je naopak $y < x$, y před x.

Uspořádání čísel podle velikosti splňuje tyto tři zřejmé zásady (principy):

I. *Žádný prvek* (*číslo*) *a není sám před sebou, t. j. nikdy není* $a < a$. (Zásada irreflexivity.)

II. *Jsou-li a, b dva různé prvky* (*čísla*), *pak vždy platí jedna*

a jen jedna z možností: *Buďto je* $a < b$ (*a menší než b*), *anebo je* $b < a$ (*b menší než a, b před a*). (Zásada dichotomie.)

III. *Jestliže a je menší než b* (*a před b*) *a b menší než c* (*b před c*), *pak je a menší než c* (*a je před c*). (*Jestliže* $a < b$, $b < c$ *potom* $a < c$.) (Zásada transitivity.)

Avšak nejsou to jen čísla nebo předměty (prvky) číselné povahy (jako ceny, velikosti a p.), které je možno uspořádat, to jest porovnat dle jistého vztahu, který můžeme obecně vyslovit rčením „x je před y" (či „x je pod y"), či „x je menší než y" a který splňuje vytčené zásady I, II, III.

Tak na př. kupující, který si vybírá z jednoho druhu výrobků, hledí si výrobky (úplně) uspořádat podle jakosti tak, aby se mohl rozhodnout pro lepší z kterýchkoli dvou výrobků. Patrně budou při takovém (úplném, dle předpokladu) uspořádání výrobků dle jakosti splněny zásady I, II, III.

Jiný příklad na „kvalitativní" uspořádání: Při hrubém a pro účely mineralogie postačujícím způsobu posuzování tvrdosti nerostů prohlašujeme za tvrdší ten ze dvou nerostů, kterým lze učinit vryp do druhého. (Dospíváme tak, jak známo, k deseti Mohsovým stupňům tvrdosti, to jest k deseti typům nerostů ve smyslu tvrdosti, viz obr. 7.

Obr. 7.

Ještě jiný příklad na „kvalitativní" uspořádání (či lépe na jednoznačnou uspořadatelnost) dává vztah subordinace v jakékoli části armády. Jak známo, musí být vždy možno jednoznačně určit (ve smyslu služebních předpisů), který z příslušníků uvažované části armády má velet ostatním, který se má ujmout velení po něm, který opět po tomto—

atd. — takže (zvláště za bojové situace) musí být vlastně předem určeno (úplné) uspořádání ve smyslu vztahu „x je (bude) podřízen y" na místě vztahu „x je menší než y". Opět jsou tu (pro vztah subordinace v armádě) splněny zásady I, II, III uvedené shora tak, jak byly vzaty z uspořádání čísel dle velikosti (to, že subordinační uspořádání je úplné, splňujíc vytčené tři zásady, je právě nutnou podmínkou akceschopnosti jakékoli části armády za jakékoli situace).

Vezměme naproti tomu v úvahu subordinační pořádek některého úřadu. Tu shledáváme jednak, že vztah „X je služebně podřízen Y" sice celkem vzato splňuje zásadu I (princip irreflexivity), t. zn. úřadní instance (zpravidla) nenařizuje sama sobě. Dále vidíme, že je vcelku dosti dobře splněna zásada III, t. j. jestliže instance X podléhá služebně instanci Y a instance Y opět služebně podléhá instanci Z, pak již je jasno, že instance X služebně podléhá instanci Z. Naproti tomu nebývá splněna zásada dichotomie II. To jest, v povaze úřadu je, že ze dvou instancí X a Y, byť kompetentních v téže záležitosti, zdaleka nikoli vždy jedna a jen jedna je úředně podřízena druhé. Nejde tedy v případě vztahu „X úředně podléhá Y" o vztah (úplného) uspořádání. Nicméně lze říci, že je (alespoň theoreticky) uznávána na místě zásady dichotomie II slabší zásada.

II*. *Je vyloučeno, aby z daných dvou prvků (různých úředních instancí) X a Y současně prvek (instance) X byl pod (úředně podléhala instanci) Y a prvek (instance) Y byl pod (úředně podléhala instanci) X.* (T. zv. zásada asymetrie.)

(T. zn., že se však může (na rozdíl od zásady II) stát, že ze dvou různých instancí ani první nepodléhá druhé, ani druhá nepodléhá první.)

Jsou-li v nějakém souboru jakýchkoli předmětů (prvků) splněny zásady I (irreflexivita), II* (asymetrie) a III (transitivita) pro nějaký pořádající vztah, pak říkáme, že daný soubor předmětů je tímto vztahem částečně uspořádán. Tak na př. tedy úřední instance (daného úřadu) tvoří částeč-

ně uspořádaný soubor ve smyslu částečného uspořádání dle vztahu úřední podřízenosti.

Příkladů na částečně uspořádané soubory jsou v denním životě spousty. Obecně každý komparativ (2. stupeň přívlastku) nám částečně uspořádává ten soubor věcí, na něž se daný přívlastek vztahuje. (Tak na př. lidé tvoří částečně uspořádaný soubor dle vztahu „X je moudřejší než Y“, kovy jsou částečně uspořádány dle vztahu „vzácnější“, úředníci dle vztahu „schopnější“, dívky dle vztahu „hezčí“, atp.) Příkladem zvláštního vztahu částečného uspořádání je vztah „x je potomkem y“.

Uspořádání (úplné) konečně mnoha předmětů (a ve zvláštních případech i nekonečně mnoha předmětů) lze si představit a graficky (geometricky) znázornit uspořádáním předmětům odpovídajících bodů na přímce (ose), na níž je vyznačen směr. (Viz na př. uspořádání typů tvrdosti nerostů na obr. 7.)

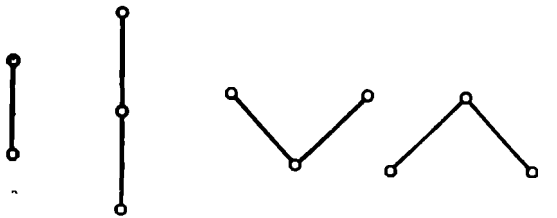
Podobně možno si představit geometricky i částečně uspořádaný soubor.[34] Místo jedné přímky (z důvodů přehlednosti svislé osy) nastupuje však celá soustava šikmých úseček, jejichž koncové body představují jednotlivé předměty uvažovaného částečně uspořádaného souboru. Okolnost, že předmět x je ve smyslu daného částečného uspořádání „před“ (či raději „pod“) předmětem y, stručně píšeme (a budeme psát) jako $x \subset y$. Tato okolnost je vyznačena prostě tím, že z bodu, představujícího předmět x, lze vést stále stoupající lomenou čáru do bodu, představujícího předmět y. (Při tom není nikterak vyloučeno, že se jednotlivé úsečky kříží.)

Čtenář se sám snadno přesvědčí, že když je obráceně dán graf, jehož nejjednoduššími součástmi jsou šikmo položené úsečky a jejich koncové body, pak tento graf vystihuje jakési částečné uspořádání; předměty budou koncové body úseček a pro dva různé body a, b lze definovat: Je $a \subset b$ tehdy a jen

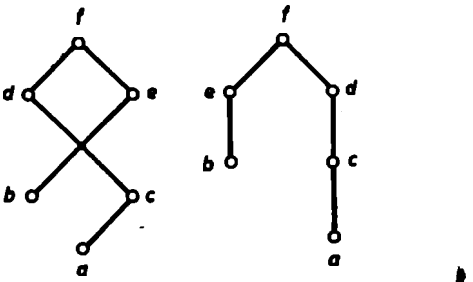
[34] Grafickému (geometrickému) znázornění částečného uspořádání se někdy říká Hasseovy diagramy.

tehdy, když z bodu a vede do bodu b stále stoupající lomená čára. (Prosté příklady jsou na obr. 9, jsou to veškery typy částečného uspořádání (t. zv. „souvislého") souboru o 2 a 3 prvcích.)

Aby se předešlo možným nedorozuměním, je dobře ke grafickému znázornění částečného uspořádání připojit několik vysvětlujících poznámek, určených zvláště pro kritického čtenáře.



Obr. 9.



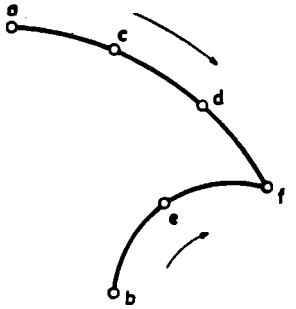
Obr. 10.

Především nechť si čtenář uvědomí, že slovní obrat pro vztah $x \subset y$ částečného uspořádání „x je pod y" (kde x a y jsou body, znázorňující (vzájemně jednoznačně) předměty z jistého částečně uspořádaného souboru) znamená méně, než to, co znamená doslova. To jest, bod a našeho grafu může ve skutečnosti při jistém způsobu nakreslení grafu být v bezprostředně názorném smyslu pod (a při jiném grafickém znázornění téhož částečného uspořádání nad) bodem b, aniž je $a \subset b$ (anebo $b \subset a$), to jest, aniž z jednoho bodu do druhého vedle stoupající lomená čára.

Za druhé je třeba si uvědomit, že jedno a totéž částečné uspořádání lze znázornit značně různými a vzájemně nepodobnými grafy. (Viz obr. 10.)

Abychom odstranili jeden zbytečný pramen této mnohoznačností v grafickém znázorňování částečně uspořádaných (konečných) souborů, vyloučíme především grafy, kde jsou některé úsečky zbytečné. Toho docílíme stanovením, že úsečkami lze spojovat body pouze „bezprostředně nad sebou" jsoucí, t. j. takové a jen takové body a a b budou spojeny *stoupající úsečkou*, pro něž je $a \subset b$ a k nimž neexistuje další c tak, že $a \subset c$, $c \subset b$. Ale ještě i po tomto stanovení zůstává v grafickém znázorňování částečného uspořádání jednak mnoho libovůle a jednak mnoho neuspokojivého. Neuspokojivé je především to, že není jasno, nakolik jsou podstatné při geometrickém znázornění částečného uspořádání oba užité pojmy „nad" a „stoupá", které vlastně (při přesné formulaci) patří do *analytické geometrie*.

Tuto nejednoznačnost a neuspokojivost lze v jistém smyslu úplně odstranit. Ukazuje se, že na geometrickém znázornění částečného uspořádání jsou charakteristické ony velmi obecné geometrické vlastnosti grafu, jež jsou předměty t. zv. *kombinatorické topologie*, o kteréžto důležité moderní matematické theorii byla zmínka na konci části o grupách. Úlohou grafu konečného částečně uspořádaného souboru je jen to, že představuje jistý systém pevným způsobem orientovaných cest (srov. výklad na konci části o grupách), při čemž je lhostejno, zda cesty (z bodu do bodu) stoupají, či klesají a zda jsou rovné, lomené či křivé (viz obr. 11). Podstatné je jen to, z kterého bodu do kterého bodu se lze dostat po souvislé a kladně probíhané cestě, procházíme-li vždy z bodu do sousedního bodu ve smyslu, který byl předem určen jako kladný, t. j. ve smyslu od x k y, kde $x \subset y$. Tyto souvislosti zůstávají právě zachovány, podrobíme-li kterýkoli graf daného, částečně uspořádaného, souboru jakékoli deformaci, jen když nic nepřetrhneme a nic, co bylo odděleno, neslepíme. (Čtenář si po způsobu z konce 1. části může představit graf částečného uspořádání nakreslen na gumové podložce.) Je tedy pojem geometrického znázornění částečného uspořádání pojmem kombinatorickotopologickým, o němž v rámci této knížky nemůžeme říci více, než těchto několik poznámek. Dodejme ještě k tomu, že kombinatoricko-topologický ráz znázornění částečného uspořádání grafem má za následek existenci zajímavých souvislostí mezi pojmem



Obr. 11.

grupy (totiž grupy cest, viz konec 1. části) a pojmem částečného uspořádání.

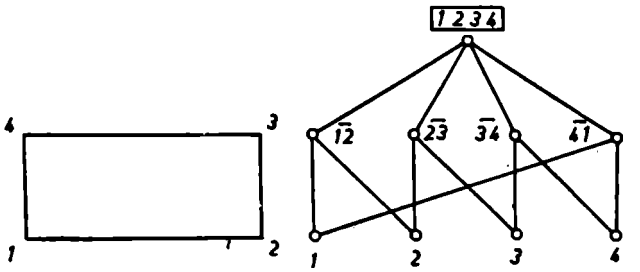
Pokud jde o samo praktické provedení grafu částečného uspořádání (konečně mnoha předmětů), je pochopitelné, že se mu snažíme dát tvar dle možnosti geometricky pravidelný, úměrný a přehledný. To jsou však požadavky účelnosti, po případě úhlednosti výkresu, které nejsou nikterak podstatně spojeny s matematickou strukturou samotného daného částečného uspořádání.

Podotkněme ještě, že shora zmíněné souvislosti theorie částečně uspořádaných souborů s kombinatorickou topologií (tato souvislost je dána zmíněnou topologickou podstatou geometrického znázornění konečného částečně uspořádaného souboru) nejsou ani jediné ani nejdůležitější. Existuje ještě docela jiná souvislost topologie s částečným uspořádáním — a to tato:

V kombinatorické topologii se často setkáváme s charakteristickým částečným uspořádáním, které je založeno na vztahu „x leží na hranici y".

Důležitost tohoto vztahu pro vystižení topologické podstaty složitějšího geometrického útvaru je snadno vidět. Je totiž zřejmo, že při spojitých deformacích geometrického útvaru zůstává vztah „x leží na hranici y" (pro součásti geometrického útvaru) zachován. Na tomto místě se musíme spokojit jen s touto hrubou zmínkou. Vztah částečného uspořádání „x leží v hranici y" je pro případ obdélníka naznačen na obr. 12 Hasseho diagramem.

Dříve, než přejdeme k výkladu pojmu svazu, je výhodné zavést ještě jeden pojem a označení. Podobně jako při (úplném) uspořádání čísel podle velikosti zavádíme t. zv. *neostré nerovniny* $a \leqq b$ (čti: a menší nebo rovno b, připouštíme tedy



Obr. 12.

i rovnost), tak i při částečném uspořádání je často vhodné spojovat obě možnosti $a \subset b$ (a pod b) a $a = b$ (a rovno b) v jediném vztahu $a \subseteq b$, který čteme: b obsahuje a (a je obsaženo v b), či obšírněji: a je pod, nebo rovno b. Vztah $\subseteq$ se nazývá polouspořádáním.

Je jasné, že vztah polouspořádání $\subseteq$ („pod nebo rovno") splňuje poněkud jiné charakteristické podmínky, než jsou ty, které splňuje vztah „ostrého částečného uspořádání" $\subset$.

Místo zásady irreflexivity I. vztahu $\subset$ nastupuje naopak zásada reflexivity vztahu $\subseteq$. Platí totiž zřejmě

I'. *Jest $x \subseteq x$ pro každé x.* (O každém x platí, že je menší nebo rovno, než x, protože je dokonce vždy x rovno x.)

Místo zásady asymetrie platí tato zásada ztotožňování:

II'. *Jestliže je $x \subseteq y$ i $y \subseteq x$, pak je $x = y$.* (Jestliže je zároveň x pod nebo rovno y i y pod nebo rovno x, pak je nutně x rovno y.)

Třetí zásada je zásada transitivity:

III. *Když je $x \subseteq y$ a $y \subseteq z$, pak je již $x \subseteq z$* (platí beze změny pro vztah $\subseteq$ stejně, jako pro vztah $\subset$).

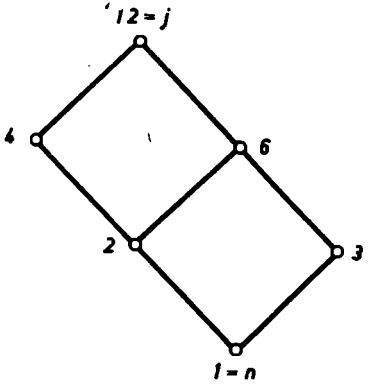
Je snadné zjistit, že každý dvojčlenný vztah, splňující I', II', III, je částečným uspořádáním, v němž je připuštěna rovnost. (Viz cvič. 2.)

To, co víme z dosavadního výkladu o pojmech částečného uspořádání a polouspořádání, nám stačí k tomu, abychom bez dalších průtahů přešli k pojmu svazu.

Vyjděme opět z dostatečně jednoduchého příkladu svazu, který je každému dobře znám. Vezměme v úvahu vztah: x je dělitelem y — v souboru všech kladných celých dělitelů čísla 12 (obr. 13). Tento vztah je zřejmě polouspořádáním, které vzniklo z částečného uspořádání podle vztahu: x je vlastním dělitelem čísla y (při čemž připouštíme za vlastního dělitele čísla y i číslo $x = 1$ pro $y \neq 1$) (viz obr. 13). Toto polouspořádání $\subseteq$ (kde tedy $x \subseteq y$ značí, že x dělí y), má tuto významnou vlastnost: Ke každým dvěma číslům (lhostejno, zda růz-

ným, či stejným) x a y (z našeho souboru, t. j. x i y jsou dělitelé čísla 12) existuje, jak známo, jednak jejich *nejmenší společný násobek*, který označme jako $x \cup y$, a jednak jejich *největší společný dělitel*, který označme jako $x \cap y$ (což obojí jsou ovšem. opět čísla z našeho souboru všech celých kladných dělitelů čísla 12). (Tak na př. píšeme: $4 \cap 6 = 2$, $4 \cup 6 = 12$.)

Nejmenší společný násobek $x \cup y$ čísel x, y splňuje tyto dva charakteristické požadavky:



Obr. 13.

(I $\cup$): *Jest* $x \subseteq x \cup y$, $y \subseteq x \cup y$. (T. j. nejmenší společný násobek, číslo $x \cup y$ je společně dělitelno číslem x i číslem y.)

(II $\cup$): *Když je* $x \subseteq z$ a $y \subseteq z$, *potom je už* $x \cup y \subseteq z$. (T. j. každý společný násobek čísel x a y má již za dělitele nejmenší společný násobek čísel x a y — číslo $x \cup y$.)

Zcela podobné jsou odpovídající požadavky, které jsou charakteristické pro největší společný dělitel $x \cap y$ čísel x, y:

(I $\cap$): *Jest* $x \cap y \subseteq x$, $x \cap y \subseteq y$. (T. j $x \cap y$ je společným dělitelem čísel x, y.)

(II $\cap$): *Když je* $z \subseteq x$ *a* $z \subseteq y$, *potom je* $z \subseteq x \cap y$. (T. j. každý společný dělitel čísel x, y je dělitelem největšího společného dělitele čísel x a y.)

Definice svazu:

Je-li nyní obecně předložen nějaký částečně uspořádaný soubor S, pak se může (ale nemusí ovšem, viz uvedené příklady částečného uspořádání) stát, že ke kterékoli dvojici x, y předmětů, či — jak budeme raději říkat — prvků ze souboru S existuje jednak prvek $x \cup y$ a jednak prvek $x \cap y$ — oba opět ze souboru S — tak, že jsou splněny požadavky (I $\cup$), (II $\cup$), (I $\cap$), (II $\cap$). V takovém případě právě říkáme (definujeme), že dané částečné uspořádání souboru S je svazové, nebo stručněji, že soubor S tvoří svaz.

Takový prvek $x \cup y$, který splňuje podmínky (I $\cup$) a (II $\cup$) bychom mohli nazývat nejmenším společným nadprvkem k prvkům x, y. Snadno nahlížíme, že takový nejmenší společný nadprvek (pokud existuje) je jen jeden jediný (ke dvěma daným prvkům x a y). Místo obšírného a nepříliš pěkného názvu nejmenší společný nadprvek nazýváme raději prvek $x \cup y$ spojením prvků x, y.

Podobně prvek $x \cap y$, který splňuje podmínky (I $\cap$) a (II $\cap$), bychom mohli nazývat největším společným podprvkem prvků x, y. (Je opět zřejmé, že takový prvek může být jen jeden.) Místo tohoto obšírného a nepěkného názvu dáváme přednost názvu průsek prvků x, y pro prvek $x \cap y$. Pro vhodnost tohoto názvosloví svědčí i jiné důvody, jež budou zřejmé, až se ukáže, že běžné geometrické spojování a protínání jakožto úkony, jimž podrobujeme přímky, body a roviny, jsou zvláštním druhem svazového spojování a protínání ve smyslu právě uvedených podmínek (I $\cup$), (II $\cup$), (I $\cap$), (II $\cap$).

Abychom se předběžně a zhruba orientovali o rozmanitosti způsobů, jimiž vystupuje pojem svazu v různých oblastech matematiky, připojme k výchozímu příkladu svazu, daného

$\left\{\begin{matrix}\text{nejmenším}\\\text{největším}\end{matrix}\right\}$ společným $\left\{\begin{matrix}\text{násobkem}\\\text{dělitelem}\end{matrix}\right\}$ tři další typické příklady svazů.

Příklad 1.

Vraťme se k pojmu (úplného) uspořádání. Je-li S libovolný uspořádaný soubor — na př. soubor racionálních čísel, kde $x < y$ značí x je menší, než y, pak položme:

za $x \cup y$ větší z čísel x, y — jsou-li to čísla různá — a číslo x, je-li $x = y$; podobně:

za $x \cap y$ menší z čísel x, y — jsou-li to čísla různá — a číslo x, je-li $x = y$.

Snadno je vidět, že se takto na každý uspořádaný soubor můžeme dívat jako na svaz, vzhledem ke vztahu polouspořádání $x \leqq y$ (menší, nebo roven). (Jsou splněny podmínky I, II*, III, pro vztah $<$ a (I$\cup$), (I$\cap$), (II$\cup$), (II$\cap$) pro spojení a průnik.)

Můžeme tedy říci: Svazové částečné uspořádání je zvláštním případem obecného částečného uspořádání. S druhé strany je však (úplné) uspořádání zvláštním druhem svazového částečného uspořádání. (Zavádí tedy svazové částečné uspořádání v jistém smyslu poněkud „lepší pořádek" než pouhé libovolné částečné uspořádání, ale zase „horší pořádek", než (úplné) uspořádání.)

Je zřejmo, že svazy — podobně jako grupy — mohou být konečné, t. j. mohou obsahovat konečně mnoho prvků, jako na př. uvedený svaz všech dělitelů čísla 12 (obr. 13), nebo mohou být nekonečné, jako na př. souhrn všech celých kladných čísel vzhledem k svazovému polouspořádání podle vztahu: x je dělitelem y.

Příklad 2.

Naznačme (zatím jen neúplně a zběžně) onen druh (nekonečných) svazů, které se vyskytují v geometrii bodů, přímek, rovin (a jejich vícerozměrných zobecnění), tedy onen důležitý druh svazů, v nichž úkony (svazového) protínání a spo-

jování mají (alespoň zčásti) svůj bezprostřední, geometrický význam.

Za prvky svazu S považujeme: Body, přímky, roviny v prostoru, k nimž pro úplnost nutno přidat ještě celý prostor a t. zv. prázdnou část prostoru. (Hned uvidíme, v čem spočívá úloha přidaných „útvarů" a proč je nutno počítat i s „prázdným útvarem".) Za polouspořádání přijmeme vztah:

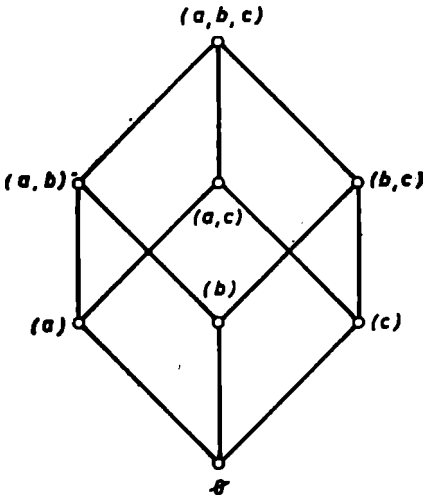
„x leží na y", který patrně splňuje podmínky I', II', III'. (x, y mohou být: Body, přímky, roviny i celý prostor, resp. jeho prázdná část.) Pak nalézáme na př., že svazovým spojením dvou různých bodů je přímka, která tyto body spojuje ve smyslu geometrickém; dále, že spojením přímky s bodem mimo ni (ve smyslu svazu) je rovina, na níž leží daný bod a daná přímka; dále, že spojením bodu s rovinou, která jej neobsahuje, je celý prostor (který jsme proto zařadili mezi prvky svazu S); že průsekem dvou protínajících se přímek je jejich průsečík. Protože jsme mezi prvky svazu S počítali i prázdnou část, kterou značme $\emptyset$, prostoru, můžeme však protínání podrobit cokoli. Tak průsekem dvou různých bodů je prázdná část prostoru a stejně je jí i průsek přímky s bodem, mimo ni ležícím. Průsekem roviny s přímkou ji protínající je průsečík této přímky s touto rovinou. Průsekem dvou protínajících se rovin je jejich průsečnice, atp.

Příklad 3.

Konečně si uveďme ještě jeden příklad konečného svazu, který je representantem důležitého druhu svazů, t. zv. Booleových algeber, jimž budeme v dalším věnovat značnou pozornost (pro aplikace, které tento druh svazů má i přímo v technické praxi). (Obr. 14.)

Z daného souboru n předmětů — na př. pro jednoduchost nechť $n = 3$ a předměty jsou a, b, c — si myslíme utvořeny všechny skupiny, které lze z daných n (= 3) předmětů vybrat — rozumí se bez opakování a bez ohledu na pořadí. *Prvky* našeho svazu B budou tedy *částečné soubory*, či prostě

části souboru (a, b, c) — při čemž za část považujeme vždy i celý soubor i t. zv. prázdný soubor (prázdnou část), neobsahující žádný předmět, t. j. obsahující 0 předmětů (prázdný soubor budeme vždy značit znakem $\emptyset$).



Obr. 14.

Za vztah svazového polouspořádání $\subseteq$ vezmeme vztah: x je částí y, při čemž písmena x a y značí části našeho daného souboru. (Přesněji: $x \subseteq y$ značí, že každý předmět z x se nalézá i v y.)[35]

Pak spojením $x \cup y$ dvou částí x, y je patrně ona část, která shrnuje předměty, obsažené v x s předměty, obsaženými v y, v jeden soubor. Průsekem $x \cap y$ dvou částí x, y je ta část obsahující právě a jen ty předměty, které jsou obsaženy

[35] Tento typický druh částečného uspořádání má jméno množinová inkluse; snadno je vidět, že splňuje zásady I′, II′, III.

jak v x tak i v y. (Tak na př. je-li $x = (a, c)$, $y = (b, c)$, pak $x \cup y = (a, b, c)$, $x \cap y = (c)$.) Doporučuji opět čtenáři, aby se sám důkladně přesvědčil, že jsou splněny požadavky I′, II′, III — jakož i podmínky (I∪), (II∪), (I∩), (II∩) (viz grafické zobrazení svazu B všech částí souboru o 3 předmětech na obr. 14). (Čtenář, který zná základy theorie množin z knížky J. Pospíšila: *Nekonečno v matematice* (sb. Cesta k vědění), ví, že se poslednímu příkladu svazu říká též t. zv. systém všech podmnožin konečné množiny o n (= 3) prvcích. V naší knížce se však zpravidla vyhýbám názvosloví theorie množin, nahrazuji slovo *množina* slovem *soubor* a slovo *prvek* slovem *předmět*, kdežto slovo prvek je vyhraženo pro prvky svazu, po případě grupy.)

Cvičení k 2,2.

1. Nakreslete si Hasseho diagram částečného subordinačního uspořádání na vašem pracovišti.

2.*Nechť $x \prec\!\!\!\cdot\; y$ značí obecně, že mezi nějakými předměty z jistého souboru S, označenými jako x a y, je jistý vztah (x a y nemusí být nutně různé předměty!). Dokažte, že jestliže platí:

I′: $x \prec\!\!\!\cdot\; x$ (zásada reflexivity);

II′: když je $x \prec\!\!\!\cdot\; y$ a $y \prec\!\!\!\cdot\; x$, pak je $x = y$ (zásada ztotožňování);

III: když je $x \prec\!\!\!\cdot\; y$ a $y \prec\!\!\!\cdot\; z$, pak je $x \prec\!\!\!\cdot\; z$ (zásada transitivity),

potom je takto již udáno jediné částečné uspořádání $\subset$ souboru S tak, že můžeme říci: Jest $x \prec\!\!\!\cdot\; y$ tehdy a jen tehdy, když je $x \subseteq y$.

3. Dokažte, že požadavky (I ∪), (II ∪) může splňovat jen jeden prvek $x \cup y$. Totéž pro (I ∩), (II ∩) a prvek $x \cap y$.

4.*Sestavte graf částečného uspořádání podle vztahu „x leží v hranici y“ pro a) úsečku, b) trojúhelník, c) čtyrstěn. Tvoří tato částečná uspořádání svazy? Jestliže nikoli — co k tomu chybí?

5.*Dokažte: Budiž S svaz. Nechť platí, že pro každý pár prvků x, y z S je spojení $x \cup y$ vždy rovno jednomu z obou prvků x a y (nebo oběma, jde-li vlastně o týž prvek (když $x = y$)). Pak S je úplně uspořádaný soubor — svazové částečné uspořádání je ve skutečnosti prostě uspořádáním. Totéž pro průnik na místě spojení. (Návod: Definuj $x < y$, když $x \cup y = y$, $x \neq y$. Dokaž I, II, III.)

6.*Dokažte, že platí

$$a \cup b = b,$$

když a jen když

$$a \cap b = a$$

přímo z definičních požadavků (I∪), (II∪), (I∩), (II∩).

2,3. POJEM SVAZU S OBĚMA ÚKONY (SPOJOVÁNÍ A PROTÍNÁNÍ) JAKO ZÁKLADNÍMI POJMY. ZÁKLADNÍ AXIOMY THEORIE SVAZŮ. PRINCIP DUALITY. POJEM ISOMORFNÍHO A HOMOMORFNÍHO ZOBRAZENÍ PRO SVAZY. POJEM ISOMORFNÍ REPRESENTACE.

Často se stává, že v daném svazu je přirozené vztah částečného (svazového) uspořádání, resp. polouspořádání (na rozdíl od prve uvedené definice svazu), považovat spíše za něco druhotného, co lze odvodit z obou pojmů spojování a protínání. Tak je tomu na př. v naznačeném geometrickém svazu, jehož prvky jsou body, přímky a roviny (spolu ještě s celým prostorem a s jeho prázdnou částí) a kde svazové spojování (protínání) se jeví rozšířením geometrického spojování (protínání). Tam je zřejmě přirozené považovat geometrické úkony spojování a protínání, resp. jejich svazové rozšíření, za prvotní pojmy, které lze zavést a charakterisovat bez výslovného užití vztahu polouspořádání „x leží na y".

Nyní půjde o to ukázat — ve smyslu úvodní poznámky k druhé části této knížky — jak svaz lze abstraktně definovat zcela podobně jako grupu. V dalším bude totiž pro nás svazem jakýkoli soubor předmětů, t. zv. prvků svazu, v němž je možno provádět (nikoli jen jeden — jako v grupě, nýbrž) jisté dva základní úkony t. zv. spojování a protínání, a to tak, že jsou splněny jisté axiomy, jež dílem připomínají některé axiomy theorie grup, dílem jsou zcela jiného druhu. Pojem svazového polouspořádání, resp. částečného uspořádání, se při tom jeví jako pojem druhotný, definovaný na základě obou základních svazových úkonů, spojování a protínání.

Vynecháme zde výslovné sledování abstrakčního pochodu, jímž bychom došli k vytčení axiomů svazu na dostatečně typickém příkladu konkretního svazu, podobně, jako jsme došli k axiomům grupy, vypozoorvaným na grupě zákrytových pohybů rovnostranného trojúhelníka. Čtenáři však doporučuji, aby si vzápětí po přečtení každého

jednotlivého svazového axiomu důkladně ověřil jeho platnost na některém z uvedených příkladů svazů.

Zato však budiž uvedeno několik poznámek, jež usnadní čtenáři orientaci v následujících základních — a později dodatečných axiomech svazu, jichž je na první pohled odstrašující množství (ve srovnání s pouhými čtyřmi, resp. pěti axiomy theorie grup). Systém axiomů svazu se však ukáže dokonale souměrným a přehledným. (Čtenář učiní dobře, když se po přehledu axiomů k těmto poznámkám vrátí.)

Jaké jsou příbuznosti a jaké typické rozdíly mezi axiomy theorie svazu a axiomy theorie grup? První dva, druhé dva a třetí dva axiomy, t. j. axiomy jednoznačnosti a neomezené proveditelnosti, axiomy asociativnosti a axiomy komutativnosti obou úkonů (t. j. spojování a protínání) jsou nám v podstatě známy jako 1., 2. a 5. axiom theorie grup. (Viz str. 9—12.) Rovněž axiom 3 theorie grup, požadující existenci jednotkového prvku v grupě, má zde dvojí obdobu (axiom 5′, 5″). Naproti tomu není u svazů ani stopy po obdobě axiomu 4. pro grupy, tohoto typického axiomu theorie grup, požadujícího existenci inversního prvku a tím i inversní úkon ke grupovému násobení, t. j. řešitelnost jistých nejjednodušších rovnic (tvaru $ax = b$, $ya = b$). Teprve ve speciálních druzích svazů, zvláště v t. zv. Booleových algebrách (které jsme již na příkladech poznali) jsou dány, jak uvidíme, různé 4. axiom theorie grup připomínající (početní) prostředky k řešení rovnic (isolování „neznámé“).

Za to však je pro svazy charakteristická úzká souvislost a podobnost mezi oběma základními svazovými úkony, spojováním a protínáním, která ovšem nemá obdoby v theorii grup. Tato souvislost je dána především t. zv. principem duality. Princip duality theorie svazů znamená toto: Jestliže v jakékoli identitě, t. j. rovnosti, platící v každém svazu jistého druhu a pro libovolné prvky nahradíme každé spojení průsekem a každý průsek spojením, pak obdržíme opět správnou identitu (t. zv. identitu duální k první), platnou opět pro libovolné prvky. Jádro principu duality je uloženo přímo v základních axiomech, jak následují. Tyto axiomy theorie svazu se totiž právě vyskytují ve dvojicích vzájemně duálních axiomů, zvlášť pro spojování a pro protínání. (Je zřejmé, že kdybychom uvedli princip duality předem jako výchozí předpoklad, stačilo by vždy uvést jen jeden z obou duálních axiomů. Je však vhodnější vtělit princip duality přímo do tvaru axiomů.) Čtenář znalý základních pojmů t. zv. *projektivní geometrie* ví, že v projektivní geometrii roviny se pod t. zv. principem duality rozumí tato zásada: Každá správná geometrická poučka přejde opět ve správnou poučku, jestliže pojem: přímka nahradíme pojmem: bod, pojem: bod pojmem: přímka, výraz: je spojením výrazem: je průsečíkem a výraz: je průsečíkem výrazem: je spojením - (a provedeme ovšem příslušné gramatické úpravy věty).

Při pozdějším doplnění základních axiomů svazu dalšími axiomy podléhá ovšem také princip duality odpovídajícímu doplnění. Tak je tomu ve svazech geometrického spojování a protínání. Princip duality projektivní geometrie je pak *důsledkem* vhodně doplněného *principu duality theorie svazů* (ve smyslu svazové povahy geometrického úkonu spojování a protínání).

Jednotlivé základní axiomy, definující pojem svazu, jsou tyto: Neprázdný soubor S jakýchkoli předmětů, t. zv. prvků, je svaz, jestliže platí:

(1′) Ke každým dvěma prvkům a, b svazu S je určen jediný prvek c z S, který se nazývá spojením prvků a s prvkem b a označuje se jako $a \cup b$.

(1″) Ke každým dvěma prvkům a, b svazu S je určen jediný prvek d z S, který se nazývá průnikem prvku a s prvkem b a označuje se jako $a \cap b$.

(Oba duální axiomy jednoznačnosti a neomezené proveditelnosti spojování a protínání.)

Pro libovolné prvky a, b, c z S platí

(2′) $(a \cup b) \cup c = a \cup (b \cup c)$.

(2″) $(a \cap b) \cap c = a \cap (b \cap c)$.

(Oba duální axiomy asociativnosti pro spojování a protínání.)

Pro libovolné prvky a, b z S platí

(3′) $a \cup b = b \cup a$.

(3″) $a \cap b = b \cap a$.

(Oba duální axiomy komutativity pro spojování a protínání.)

Pro libovolné prvky a, b, c z S platí

(4′) $a \cup (a \cap b) = a$.

(4″) $a \cap (a \cup b) = a$.

(Oba duální axiomy absorbce („pohlcování“).)

Jak již řečeno, oba dva poslední axiomy jsou typické pro svazy. Kdežto není třeba zvláště vykládat smysl axiomů (1′) až (3″), neškodí popsat několika slovy význam axiomů absorbce (4′) a (4″). Tyto axiomy říkají: Spojení (průnik) daného prvku s průsekem (spojením) tohoto prvku a libovolného dalšího prvku dá zpět daný prvek. Jako by tedy vskutku průsek dvou prvků byl pohlcován každým ze svých činitelů, t. j. jako by průsek zanikal ve spojení se svým činitelem; duálně k tomu jako by vskutku spojení zanikalo (bylo pohlceno) jsouc protato svým činitelem.

Co se týče početního významu axiomů absorbce, je jasné, že tkví v zjednodušování složených výrazů pro prvky svazu. Svou ryze početní úlohou tedy axiomy absorbce připomínají pravidla o vytýkání, resp. o krácení (čísel). Jako těchto pravidel — i oněch se dá někdy použít k takové úpravě rovnosti ve svazu, po níž žádaný prvek zůstane isolován na jedné straně („řešení rovnice"). Nahlédneme, jak se užívá axiomu absorbce na důkazu jisté dvojice duálních zásad, která je důsledkem uvedených základních svazových axiomů (1′)—(4′) a kterou se tak ostře odlišují svazy od grup.

Věta:

Pro každý prvek a svazu S platí

$$a \cup a = a, \quad a \cap a = a.$$

(T. zv. zásada idempotentnosti spojování a protínání.[36])

Důkaz:

Položme (při libovolně daném prvku a z S) $a \cup a = c$. (Užito axiomu (1′). Položme $b = c$ v axiomu (4′). Dostáváme

$$a = a \cup (a \cap c) = a \cup (a \cap (a \cup a)) \ldots (+).$$

Z axiomu (4″) (porovnáním prvního se třetím členem v rovnostech (+) plyne

[36] Někdy bývá tato zásada považována za axiom (v jiných systémech axiomů theorie svazů).

$$a \cap (a \cup a) = a.$$

Nahrazením a za $a \cap (a \cup a)$ v (+) vskutku plyne

$$a = a \cup a.$$

Rovnost $a = a \cap a$ se dokáže duálním způsobem, což přenechávám čtenáři jako cvičení.

Zásada idempotentnosti říká, že ačkoli bychom na podkladě axiomů asociativnosti mohli (podobně jako v grupách) definovat

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

(a duálně pro opakované protínání namísto spojování), k ničemu by to nebylo, protože bychom měli

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

Vraťme se k základním svazovým axiomům (1′) až (4″); nelze již odkládat splacení dluhu z předchozího paragrafu, v němž byl pojem svazu zaveden na podkladě částečného uspořádání. Je třeba ukázat, že jde o jeden a týž pojem svazu, t. j. předně: *Platí-li* (v souboru S) *axiomy* (1′) *až* (4″), *pak je tím již jednoznačně určen jistý vztah částečného uspořádání* $\subset$ (ve smyslu zásad I, II$^+$, III), resp. odpovídající vztah polouspořádání $\subseteq$ (ve smyslu I′, II′, III) *a to tak, že výsledky spojování a protínání, zavedeného tímto částečným uspořádáním podle podmínek* (I$\cup$), (II$\cup$), (I$\cap$), (II$\cap$), *jsou tytéž, jako při spojování a protínání původně daném.* A za druhé, obráceně: *Jakmile je spojování a protínání zavedeno pomocí částečného uspořádání podle podmínek* I, II$^+$, III, (I$\cup$), (II$\cup$), (I$\cap$), (II$\cap$), *pak jsou již splněny axiomy* (1′) až (4″) — *a navíc, pak částečné uspořádání definované pomocí právě zavedeného spojování (nebo protínání) je totožné s tím, z něhož jsme vyšli.*

Důkaz první poloviny tvrzení:

Zaveďme tento dvojčlenný vztah „$\subset$“: Pro prvky a, b svazu S (svazu ve smyslu axiomů (1′)—(4″)), budiž $a \subset b$, když a jen když je

$$a \cup b = b,\ a \neq b.$$

Máme ukázat, že tento vztah „$\subset$" je hledaným částečným uspořádáním. Pro „$\subset$" je zřejmě splněna zásada irreflexivity I. Dokažme, že je pro „$\subset$" splněna i zásada asymetrie II+. Skutečně, kdyby bylo současně $a \cup b = b$, $a \neq b$ čili $a \subset b$ a $b \cup a = a$, $b \neq a$ čili $b \subset a$, pak dle axiomu komutativity (3'), $a \cup b = b \cup a$ by bylo $a = b$, což jsme (předpokladem) vyloučili.

Konečně ukažme splnění zásady transitivnosti (III) naším vztahem $\subset$. Nechť je tedy $a \subset b$ a $b \subset c$ čili nechť platí $a \cup b = b$, $b \cup c = c$, $a \neq b$, $b \neq c$. Máme odvodit $a \subset c$. Dosazením z dané první rovnosti do druhé máme $(a \cup b) \cup c = c$ a užitím axiomu asociativnosti (2') a druhé z daných rovností máme $a \cup c = c$. Při tom nemůže být $a = c$, protože jinak bychom z daných rovností měli $a = b$ proti předpokladu. Tedy je skutečně $a \subset c$.

Že výsledky jak spojování tak protínání, zavedeného pomocí právě určeného vztahu částečného uspořádání čili jím daného polouspořádání jsou totožné s původně (přímo) daným spojováním a protínáním, to je již nyní bezprostředním důsledkem definice našeho částečného uspořádání. (Radím však čtenáři, aby nedůvěřoval tomuto ujištění a sám se přesvědčil.) — Tím je první polovina tvrzení dokázána.

Důkaz druhé poloviny tvrzení:

Když je svaz definován pomocí částečného uspořádání (zásadami I, II*, III, (I$\cup$), (II$\cup$), (I$\cap$), (II$\cap$), pak předně jsou splněny axiomy (1'), (1''), (3', (3''). Dále axiomy asociativnosti (2') a (2'') odvodíme dále takto: Jsou-li a, b, c prvky svazu, definovaného pomocí částečného uspořádání, položme

$$(a \cup b) \cup c = h,\ a \cup (b \cup c) = k.$$

Dle zásady (I$\cup$) je (dle druhé rovnosti) $a \subseteq k$ a $b \cup c \subseteq k$. Poslední však (dle téže zásady) má za následek $b \subseteq k$ a $c \subseteq k$. Avšak $a \subseteq k$ a $b \subseteq k$ dává $a \cup b \subseteq k$ dle zásady (II$\cup$). Toto spolu s $c \subseteq k$ dává $h \subseteq k$ opět dle zásady (II$\cup$). Zcela stejným

způsobem se odvodí $k \subseteq h$. Dohromady tedy $k = h$, dle zásady ztotožňování II', což se mělo dokázat.

Konečně axiomy (4'), (4") absorpce odvodíme takto:

Označme $d = a \cup (a \cap b)$. Pak je dle (I $\cup$) $a \subseteq d$. Dále dle (I $\cap$) je $a \cap b \subseteq a$. Z posledního však pomocí I' přes $a \subseteq a$ již dostáváme dle zásady (II $\cup$) $d \subseteq a$. Dohromady tedy (dle zásady ztotožňování II') $a = d$, což je axiom (4'). Axiom (4") se odvodí duálním způsobem, což přenechávám čtenáři.

Tím je dokončen důkaz celého tvrzení o logické rovnocennosti obou definic svazu, totiž dříve uvedené, názornější definice pomocí pojmu částečného uspořádání a později uvedené definice pomocí axiomů pro úkony spojování a protínání.

A ještě jedna často užitečná *poznámka*:

Z počítání číselnými nerovninami známe toto pravidlo o „sečítání nerovnin": Když je $a \leqq b$ a $c \leqq d$, pak je i $a + c \leqq b + d$.

Zcela obdobné — a sice hned (následkem principu duality) dvojí pravidlo (pro „spojování nerovnin" a pro „protínání nerovnin" máme i ve svazech.

Čtenář si sám ověří (viz cvič. 3), že ze dvou „nerovnin" $a \subseteq b$ a $c \subseteq d$ v libovolném svazu plyne jednak „nerovnina" $a \cup c \subseteq b \cup d$ a jednak nerovnina $a \cap c \subseteq b \cap d$.

Doplňme věc ještě poznámkou, že stejné částečné uspořádání $\subset$ o němž byla právě řeč, možno ve svazu, daném přímo pomocí spojování a protínání zavést podmínkou: $a \subset b$ tehdy a jen tehdy, když $a \cap b = a$, $a \neq b$. To již není třeba dokazovat, protože plyne z principu duality, o němž byla řeč svrchu. (Čtenáři však neuškodí, provede-li si ze cvičných důvodů podrobně celé odvození zvlášť pro tento duální případ.)

Abychom měli na očích alespoň jeden příklad na užití právě dokázaných souvislostí, připomeňme si znova již zhruba naznačený geometrický svaz, daný všemi body, přím-

kami a rovinami (včetně celého prostoru a jeho prázdné části). Zde nám právě dokázané tvrzení ukazuje, jak geometrický vztah „x leží na y" je *odvozeným vztahem*, který je (jako jediný možný) určen za pomoci spojování předpisem „spojení x s y je samo y". — Stejně tak dobře možno však říci pomocí protínání duálně: „x leží na y" znamená právě tolik, co „x se s y protíná v samém x" (viz cvič. 3).

Probrali jsme základní axiomy theorie svazů (1′) až (4″) a jejich souvislost s pojmem částečného uspořádání. Uvedené čtyři dvojice základních axiomů však ještě necharakterisují dostatečně na př. geometrické spojování a protínání, což kritický čtenář musel shledávat neuspokojivým. Ty druhy svazového spojování (a protínání), které byly dosud v příkladech uvedeny, jsme pomocí axiomů 1′ až 4″ charakterisovali jen velmi nedokonale. Kdyby axiomatická abstraktní methoda theorie svazů nebyla s to na př. vystihnout z podstaty spojování a protínání částí (množin) či z úkonů geometrického spojování a protínání více než to, co jsme vytkli shora, byl by pojem svazu pouhou abstraktní ilustrací známých matematických pojmů bez většího samostatného významu. Na štěstí však jednotlivé zvláštní a častěji se vyskytující druhy svazů dovedeme dobře vystihnout a odlišit. Ovšem k přesnějšímu vystižení toho či onoho druhu svazových úkonů je potřeba *dalších axiomů*. I v tom je tedy rozdíl oproti theorii grup: Kdežto abstraktní theorie grup je s to podat hluboké matematické poznatky na podkladě pouhých čtyř (po případě pěti, pokud jde o Abelovy grupy) axiomů, základní axiomy theorie svazů (alespoň při současném stavu matematiky) tvoří ještě příliš všeobecný a málo uzavřený systém, který (za současného stavu theorie) sám nestačí jako podklad hlubších úvah.

Předně doplňme ještě základní a všeobecné axiomy theorie svazů jistou dvojicí vzájemně duálních axiomů 5′ a 5″, které jsou naprostou obdobou 3. axiomu theorie grup (o jednotkovém prvku), třebaže nemají té zásadní důležitosti.

Pojem jednotky a nuly svazu:

5′	5″
Existuje jediný prvek j, t. zv. jednotkový prvek svazu, či stručněji jednotka svazu tak, že je	Existuje jediný prvek n, t. zv. nulový prvek svazu, či stručněji nula svazu tak, že je
$j \cap a = a,\ j \cup a = j$	$n \cup a = a,\ n \cap a = n$
pro každý prvek a ze svazu.	pro každý prvek a ze svazu.

Na příklad ve svazu (Booleově algebře) všech částí (konečného) souboru (viz na př. obr. 14) je jednotkovým prvkem celý (plný) soubor, nulovým prvkem prázdný částečný soubor. Podobně ve svazu geometrického spojování a protínání je jednotkovým prvkem celým prostor a nulovým prvkem jeho prázdná část. Existují ovšem svazy, které postrádají buď jednotky nebo nuly nebo obojího. Na př. ve svazu všech celých kladných čísel, jehož svazovým polouspořádáním je vztah dělitelnosti, je nulovým prvkem číslo 1, kdežto jednotkový prvek neexistuje. Když zavedeme vztah x je dělitelem y — pišme opět $x \subseteq y$ — mezi kladná racionální čísla tak, že klademe $x \subseteq y$ tehdy a jen tehdy, když existuje celé kladné číslo z tak, že $z \,.\, x = y$, pak takovýto vztah dělitelnosti je opět svazovým polouspořádáním. Daný svaz racionálních čísel postrádá jak jednotky, tak i nuly. Takový nedostatek však (na rozdíl od theorie grup), není ve svazech žádným neštěstím. Chybějící jednotku (nulu) svazu možno prostě uměle přidat, aniž bychom jinak byli nuceni měnit již stávající úkony spojování a protínání. Tak na př. chceme-li, aby shora zmíněný svaz všech celých kladných čísel ve smyslu vztahu dělitelnosti se změnil ve svaz s jednotkovým prvkem, můžeme přidat t. zv. „kladné nekonečno“ $+\infty$ jako nový prvek, stanovíce (pro úplnost), že „číslo“ $+\infty$ je dělitelno každým číslem celým; pak zřejmě bude $+\infty = j$ jednotkovým prvkem takto pozměněného (rozšířeného) svazu celých čísel (kde spojení = nejmenší spol. násobek, průnik = největší spol. dělitel tak, jako dříve).

Je obecně zřejmo, že jednotka svazu je vždy nejvyšším („největším"), nula svazu nejnižším („nejmenším") prvkem ve smyslu svazového částečného uspořádání — pokud obě existují. Zřejmě každý konečný svaz má nulu i jednotku, jakožto průnik, resp. spojení všech svých (t. j. konečně mnoha) prvků. (Je třeba si uvědomit, že se tu opíráme o oba axiomy asociativnosti $2'$, $2''$ pro svazové spojování a protínání, které nám teprve umožňují jednoznačně zavádět spojení a průnik libovolného konečného počtu prvků svazu „najednou".)

Isomorfní a homomorfní zobrazení v theorii svazů.

Všeobecné pojmy z theorie svazů je třeba dále doplnit přenesením pojmů *isomorfní*, (*homomorfní*) *zobrazení* a „abstraktní" svaz, lépe: typ isomorfismu svazu — z theorie grup, kde jsou nám známy — na *theorii svazů*.

Stejně, jako v theorii grup i v theorii svazů isomorfním zobrazením svazu S na svaz S^* rozumíme takové vzájemně jednoznačné přiřazení φ prvků z S prvkům z S^*, že platí

$$\varphi(x \cup y) = \varphi(x) \cup \varphi(y),$$
$$\varphi(x \cap y) = \varphi(x) \cap \varphi(y).$$

(Zobrazení φ přenáší spojení i průnik z S na S^*; zhruba řečeno, ve svazech S a S^* se spojuje a protíná „v podstatě" stejně.) Jako v grupách pak říkáme, že svazy S a S^* jsou (navzájem) *isomorfní*.

Prostý příklad isomorfního zobrazení svazu na svaz je toto: (Bohatší příklady viz na konci odst. 2,8.)

S budiž svaz všech částí daného, konečného počtu n předmětů, pro jednoduchost na př. přirozených čísel, $1, 2, 3, \ldots, n$. (Viz str. 125—7.)

S^* budiž svaz všech dělitelů čísla $2 \cdot 3 \cdot 5 \ldots p_n = N$ (prvních n po sobě (dle velikosti) následujících prvočísel) — ve smyslu svazového polouspořádání dle vztahu dělitelnosti.

φ nechť přiřazuje dané skupině k různých čísel, t. j. prvku $(x = (i_1, i_2, \ldots, i_k)$ ze svazu S součin těch prvočísel, jejichž místa v posloupnosti prvočísel (dle velikosti) jsou právě celá kladná čísla $i_1, i_2, \ldots, i_k$. Toto číslo tedy označíme jako $x^* = \varphi(x)$.

Čtenář si sám snadno uvědomí, že zobrazení φ je isomorfním zobrazením svazu S na svaz S^*. (Nejmenší společný násobek $x^* \cup y^*$ dvou dělitelů x^* a y^* čísla $2 \cdot 3 \cdot 5 \ldots p_n$ tvoříme patrně totiž tak, že shrneme prostě prvočíselné činitele obou čísel x^* a y^* v jeden součin; podobně největší společný dělitel $x^* \cap y^*$ dvou dělitelů čísla $2 \cdot 3 \cdot 5 \ldots p_n$ se utvoří jako součin těch prvočísel, jež jsou činiteli zároveň v x^* i v y^*.) Další příklady na isomorfní zobrazení svazu na svaz najde čtenář ve cvičeních (viz též obr. 14). Je-li φ isomorfní zobrazení svazu S na svaz S^*, pak je $x \subseteq y$ v S (ve smyslu svazového polouspořádání) tehdy a jen tehdy, když je $\varphi(x) \subseteq \varphi(y)$ v S^*, protože je $x \cup y = y$ v S tehdy a jen tehdy, když je $\varphi(x) \cup \cup \varphi(y) = \varphi(y)$ v S^*. Z toho vyplývá, že jednotce a nule j a n svazu S odpovídají jednotka a nula j^* a n^* svazu S^*, t. j. $\varphi(j) = j^*$, $\varphi(n) = n^*$ při každém isomorfním zobrazení φ svazu S na svaz S^*. Tak v předchozím příkladě $n = \emptyset$ (prázdná část), $\varphi(\emptyset) = 1$,[37] $j = (1,2, \ldots n)$ φ (j)$=N$

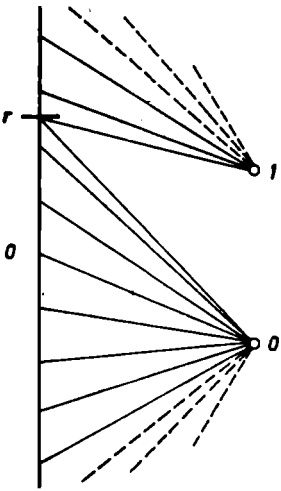
Jestliže od zobrazení svazu S na svaz S^* požadujeme vše, co prve, jenom nikoli nutně to, aby přiřazení bylo vzájemně jednoznačné, t. j. jestliže připustíme, že některý prvek z S^* může být obrazem více než jednoho prvku z S, pak říkáme, že zobrazení S na S^* je homomorfní. Homomorfní zobrazení svazu na svaz je tedy, stejně jako při grupách, jakési promítnutí svazu na svaz, které rovněž přenáší spojování a protínání (z S na S^*), ale jen v jednom směru, tedy nikoli věrně.

Abychom měli jednoduchý a dosti známý příklad, vezměme si za svaz S dle velikosti uspořádaný soubor všech racionálních čísel, seřazených podle velikosti na svislé číselné ose (záporná část budiž dole, kladná nahoře), za svaz S^* (v šech obrazů) si vezměme nejjednodušší uspořádaný soubor (obsahující více než jediný předmět), totiž soubor čísel 1 a 0. Budiž r nějaké pevně zvolené reálné číslo (t. j. desetinný zlomek, jehož jednotlivé číslice na libovolném místě desetinného

[37] Čtenáře nesmí mást, že „nulou" svazu S^* je tu číslo 1.

rozvoje lze vždy určit, aniž se však nutně jakékoli cifry musí periodicky opakovat). Jako homomorfní zobrazení svazu S na svaz S^* pak máme toto přiřazení φ_r:

Všem racionálním číslům, větším nebo rovným reálnému číslu r, přiřadíme číslo 1, t. j. $\varphi_r(x) = 1$ pro $x \geqq r$. A všem racionálním číslům ostatním přiřadíme číslo 0, t. j. $\varphi_r(x) = 0$ pro $x < r$. Pak φ_r je homomorfní zobrazení svazu S na svaz S^*, které lze znázornit skutečným geometrickým promítáním (viz obr. 15). Přenechávám čtenáři jako lehké a užitečné cvičení podrobný důkaz, že shora vytčené podmínky pro to, aby dané zobrazení bylo homomorfní, jsou skutečně splněny.



Obr. 15.

(Dá se dokonce ukázat, že každé homomorfní zobrazení právě uvedeného svazu S na svaz S^* je vytvořeno podobným způsobem jistým reálným číslem. Reálná čísla bychom mohli přímo definovat jako homomorfní zobrazení uspořádaného svazu S racionálních čísel na uspořádaný svaz $S^* = (0, 1)$. To je v podstatě známá t. zv. Dedekindova definice reálného čísla řezem.)

Dodejme ještě k pojmu homomorfního zobrazení svazu na svaz, s nímž se čtenář setká ještě v dalších výkladech a ve cvičení toto:

Kdežto u grup nás pojem homomorfního zobrazení vedl k důležitému pojmu normální podgrupy, při čemž se ukázalo, že znát všechny normální podgrupy dané grupy je rovnocenné se znalostí všech homomorfních obrazů dané grupy (až na isomorfismus ovšem, viz 1. věta o isomorfismu theorie grup, str. 72), není žel nic podobného u svazů v obecném případě. Definujeme sice pojem podsvazu daného svazu (stejně jako

pojem podgrupy) jakožto (neprázdný) soubor prvků z daného svazu vybraných, do něhož se dvěma prvky náleží i jejich spojení a průnik. (V případě, že daný svaz má jednotku, resp. nulu, žádáme zpravidla, aby je i podsvaz obsahoval.) Ale obdoba normální podgrupy tu chybí, s výjimkou některých zvláštních druhů svazů (na př. zmíněných Booleových algeber).

A ještě dvě srovnání abstraktní theorie grup s abstraktní theorií svazů.

Stejně jako v abstraktní theorii grup jsou naším vlastním předmětem v abstraktní theorii svazů nikoli přímo jednotlivé svazy, nýbrž hned celé *typy* (třídy) *svazů vzájemně isomorfních*. To znamená, že — podobně jako v abstraktní theorii grup — nezáleží anina konkretní povaze (definicích) jednotlivých prvků svazu, ani na tom, jakým způsobem se uskutečňuje (vyhledává) spojení a průnik daných dvou prvků svazu. Záleží jen na počtu od sebe odlišených prvků a na pouhých výsledcích svazových úkonů, to jest na tom, co se pomocí isomorfního zobrazení přenáší z jednoho svazu na druhý. Dva isomorfní svazy považujeme ve smyslu abstraktní theorie svazů za naprosto rovnocenné — se všemi výhodami logické přesnosti a obecnosti takovéhoto pojímání, jak to bylo zdůrazněno na příslušném místě při grupách.

Stejně jako v abstraktní theorii grup hledíme však i v theorii svazů vyvažovat a doplňovat methody abstrakce (axiomatisace) obráceným postupem konkretisace. To jest, hledáme isomorfní representace všech možných abstraktních svazů axiomaticky charakterisovaného druhu vhodným konkretním svazem, hledáme uskutečnění logicky možných svazových úkonů určitým způsobem jejich skutečného provádění. Avšak ani v případě konečných svazů, následkem jejich příliš veliké rozmanitosti, nemáme dostatečně universální a při tom dostatečně konkretní druh svazového spojování a protínání, který by hrál obdobnou úlohu, jako násobení matic při vystihování grupového násobení. Prostředky a způsob representace svazů jsou dosti složité a vzájemně se

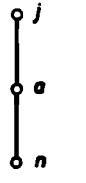
značně liší podle dodatečných axiomů, charakterisujících jednotlivé druhy svazů. Seznámíme se později s nejjednoduššími z nich, to jest s t. zv. množinovou representací konečné Booleovy algebry.

Společné je všem representacím v theorii svazů toto: Prvky representujících svazů jsou *zpravidla* jisté soubory čili množiny matematických předmětů, při čemž, je-li $x \subseteq y$ ve smyslu representovaného svazu, je množina, representující prvek svazu x obsažena v množině, representující prvek svazu y.[38] (Avšak za matematické prostředky, kterých je třeba užít k definici representujících *svazových úkonů* spojování a protínání se obecně nikterak nehodí jednoduché t. zv. sjednocování a pronikání množin (viz 2,4). Jsou to prostředky někdy poněkud složité. (Patří buď do abstraktní algebry nebo do t. zv. množinové topologie a vymykají se z rámce této knížky.)

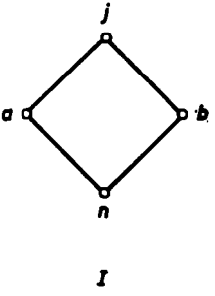
S hlediska abstraktní theorie svazů bychom mohli výsledky svazového spojování a protínání (alespoň především u konečných svazů o nepříliš velikém množství prvků) zanášet do tabulky, podobně jako jsme to činili u grup. (Viz str. 8.) (Tabulky by byly ovšem dvě, zvlášť pro spojování a zvlášť pro protínání.)

Užíváme však raději přehlednějšího grafického znázorňování, o němž jsme již hovořili. Na obr. 16, 17, 18, 19 jsou znázorněny všechny abstraktní svazy o 2, 3, 4 a 5 prvcích. (T. j.

Obr. 16.



Obr. 17.



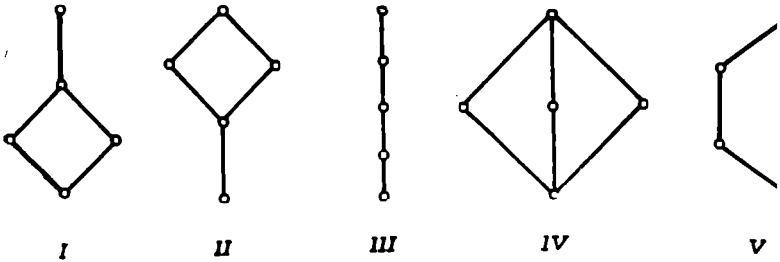
Obr. 18.

[38] Polouspořádání representovaného svazu přechází tedy v *množinovou inklusi*, což ale nijak neznamená, že by spojování a protínání svazu přešlo v pouhé množinové spojování a protínání.

každá třída vzájemně isomorfních svazů je vlastně representována jedním konkretním (ve smyslu grafické geometrické representace svazem).

Počet vzájemně neisomorfních svazů o daném počtu prvků silně stoupá. (Je již 15 svazů o 6 prvcích: radím čtenáři, aby si nakreslil graf aspoň některého z nich. (Cvič. 5.))

Tím jsme skončili část, jednající o obecném pojmu svazu. Dále si blíže všimněme jen jednoho důležitého zvláštního druhu svazů: t. zv. *Booleových algeber*.



Obr. 19.

Cvičení k 2,3.

1. Dokažte zásadu idempotentnosti pro průnik.

2. Odvoďte axiom 4″ (druhý axiom absorbce) ve svazu, daném částečným uspořádáním, t. j. daném požadavky I, II⁺, III, (I ∪), (I ∩),(II ∪), (II ∩).

3. Ukažte, že ve svazu ve smyslu axiomů 1′ až 4″ lze částečné uspořádání zavést definicí:

$$a \subset b, \text{ když } a \cap b = a,\ a \neq b.$$

(Ukažte, že toto částečné uspořádání je totožné se svazovým částečným uspořádáním, daným stanovením v textu.)

4. Položme pro dvě *racionální* čísla x, y *kladná* $x \subseteq y$ tehdy a jen tehdy, když existuje *celé* kladné číslo z tak, že je $x \,.\, z = y$. Dokažte, že tento vztah „$\subseteq$" je svazovým polouspořádáním (že tedy racionální kladná čísla tvoří (nekonečný) svaz v polouspořádání podle dělitelnosti).

Znázorněte toto svazové částečné uspořádání graficky pro podsvaz racionálních čísel tvaru $2^k 3^l$ $(k, l = 0, \pm 1, \pm 2, \pm 3, \ldots)$.

5.* Udejte všech 15 typů svazů o 6 prvcích (ve formě grafu).

2,4. AXIOMY DISTRIBUTIVITY A DOPLŇKU. POJEM BOOLEOVY ALGEBRY. MNOŽINOVÉ SPOJOVÁNÍ A PROTÍNÁNÍ.

Vraťme se k příkladu svazu všech vybraných skupin (čili částí ze souboru (čili jak se matematice říká, *množiny*) tří různých předmětů a, b, c — (včetně skupiny prázdné $\emptyset = n$ a skupiny plné $(a, b, c) = j$). (Svazové úkony jsou nám již známé a jsou graficky vyznačeny na obr. 14.)

Tento svaz má $2^3 = 8$ prvků. Kdybychom se obecněji zabývali svazem všech skupin, které lze vytvořit z n daných předmětů $a_1, a_2, \ldots, a_n$, pak bychom určili snadno, že počet prvků tohoto svazu (t. j. počet řečených skupin) je 2^n. (Z n předmětů můžeme totiž vybrat, jak se čtenář pamatuje ze školy, $\binom{n}{k}$ skupin o k předmětech, kde

$$\binom{n}{k} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{1 \cdot 2 \ldots k}$$

je známý binomický koeficient. Pak dle binomické poučky je

$$2^n = (1+1)^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}.$$)

V takovémto svazu, čili, jak říkáme a budeme říkat a psát: *v Booleově algebře B_n všech částí konečného souboru* (*množiny*) *o n (= 3) předmětech je spojení dvou prvků* (t. j. částí), *dáno části, která obsahuje právě a jen předměty, jež patří aspoň do jedné ze spojových částí. Průsek* dvou prvků (t. j. částí) *je pak část, obsahující právě a jen ty předměty, jež patří současně do obou protínaných částí.*

Půjde nám nejprve o to nalézt, jakými specifickými vlastnostmi je toto t. zv. *množinové spoje* čili *sjednocení a množinový průnik* čili *průnik* obdařeno, jaké jsou proně splněny další axiomy.

Čtenář si jistě dobře vzpomene na „samozřejmý" zákon, jímž se řídíme při kombinovaném sečítání a násobení čísel (at

již jde o konkretně numericky daná čísla nebo o čísla, označená písmenky), totiž na t. zv. zásadu distributivity sečítání vůči násobení, prostěji řečeno, na zásadu vytýkání před závorku ze součtu. Tato zásada je dána identitou

$$x \,.\, (y + z) = x \,.\, y + x \,.\, z$$

(platnou pro každé x, y, z). (Násobek součtu je roven součtu násobků jednotlivých sčítanců.)

Mysleme si na okamžik, že písmenka x, y, z znamenají nějaké prvky Booleovy algebry B_n (uvažme pro určitost $n = 3$, $x = (a, b)$, $y = (b, c)$, $z = (a, c)$) — to jest nějaké části (skupiny) vybrané z daných n předmětů. Dále si nahraďme znak „." pro násobení znakem „$\cap$" pro průnik a znak „+" pro sečítání znakem „$\cup$" pro spojování.

Pak platí v B_n identická rovnost, která se formálně nijak neliší od zákona distributivity. (V našem př. máme

$$(a, b) \cap [(b, c) \cup (a)] =$$
$$= [(a, b) \cap (b, c)] \cup [(a, b) \cap (a)]$$

to jest

$$(a, b) \cap (a, b, c) = (a, b) = (b) \cup (a).)$$

Obecněji nalézáme splnění následujících dvou vzájemně duálních axiomů distributivity v takovýchto Booleových algebrách B_n:

Jsou-li x, y, z libovolné prvky, pak platí

6′	6″
$x \cap (y \cup z) =$	$x \cup (y \cap z) =$
$= (x \cap y) \cup (x \cap z).$	$= (x \cup y) \cap (x \cup z).$

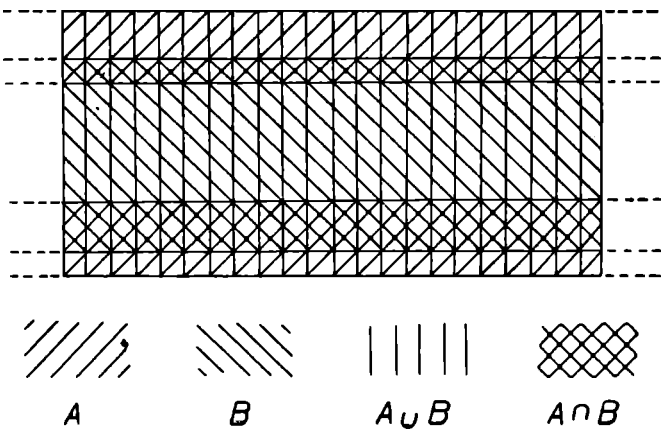
Svaz, v němž platí oba axiomy 6′ a 6″ se nazývá distributivním svazem.

Typické příklady distributivních svazů jsou právě ty svazy, jejichž prvky jsou jisté (nikoli obecně všechny) *části* (podmnožiny) *daného souboru* (množiny) a kde je spojování a protínání dáno *množinovým způsobem* tak jako ve svazu B_n). (Prvky uvažovaných svazů mohou být obecně ovšem částí konečné nebo nekonečné.)

Takovým svazům, jejichž prvky jsou (nějaké) části dané množiny (souboru předmětů) a v nichž všechna spojení i všechny průseky jsou sjednocení a průniky, množin se říká množinové okruhy. Uveďme alespoň dva příklady na množinové okruhy.

4. příklad: Prvky svazu nechť jsou všechny konečné části (soubory předmětů) vybrané z daného nekonečného souboru, na př. všechny konečné soubory (části množiny) přirozených čísel. Dostáváme tak *množinový okruh* všech *konečných* částí *nekonečné množiny*. sjednocení dvou konečných částí je ovšem konečná část — a tím spíše to platí pro průnik; tento svaz (množinový okruh) nemá jednotku svazu.)

5. příklad: Za prvky našeho svazu, t. j. množinového okruhu, vezměme ty části roviny (t. j. části množiny všech bodů roviny), které jsou uvnitř jednoho nebo několika) vodorovných pásů (viz obr. 20) (rovnoběžných s osou x). (Každá taková konečná sku pina pásů představuje jistou část roviny ležící uvnitř uvažovaných pásů. Tedy body ležící na přímkách pásy omezu jících do našich částí roviny nepatří.) Pak sjednocení dvou takovýchto pásových částí roviny je opět takovou pásovou částí roviny, kde pásy — rozumí se, že v konečném počtu — vzniknou tak, že dva do sebe zapadající pásy splynou v jeden širší pás a pásy od ostatních oddělené se prostě přidají. Průnik dvou takovýchto částí roviny je opět takovouto částí roviny, který se bude patrně skládat ze všech užších pásů, tvořících spo-



Obr. 20.

lečnou část vždy některých dvou pásů z jedné a druhé z našich částí roviny (t. j. jedné a z druhé skupiny pásů).

Dokažme si obecně, že *množinové okruhy jsou distributivními svazy*. Buďtež tedy obecně dány libovolně tři prvky množinového okruhu X, Y, Z (t. j. části jakési výchozí množiny). Pak tvrdíme, že části $X \cap (Y \cup Z)$ a $(X \cap Y) \cup (X \cap Z)$ z nich utvořené jsou si rovny (t. j. vše, co patří do jedné, patří i do druhé množiny — a obráceně). Rovněž tak jsou si rovny části $X \cup (Y \cap Z)$ a $(X \cup Y) \cap (X \cup Z)$.

Dokažme jen první z obou rovností (druhá se dokáže duálně). Nejprve tedy nechť předmět x je obsažen v části $X \cap (Y \cup Z)$. T. j., x je v X a zároveň aspoň v jedné z obou množin Y, Z. Pak zřejmě x je obsaženo buď současně v X i v Y, nebo je současně obsaženo v X i v Z (nebo v obojím). Tedy je zřejmě

$$X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z) \quad *) \qquad (a)$$

Naopak však platí (v každém svazu vždy) nerovniny $X \cap Y \subseteq X$ a $X \cap Z \subseteq X$, takže jejich spojením (viz pozn. na str. 134) a na základě zásady idempotentnosti (str. 131) máme

$$(X \cap Y) \cup (X \cap Z) \subseteq X \cup X = X. \qquad (+)$$

Dále je ovšem i $X \cap Y \subseteq Y$ a $X \cap Z \subseteq Z$, takže spojením těchto nerovnin máme

$$(X \cap Y) \cup (X \cap Z) \subseteq Y \cup Z. \qquad (++)$$

Protětím nerovnin $(+)$ a $(++)$ máme pak nerovninu

$$(X \cap Y) \cup (X \cap Z) \subseteq X \cap (Y \cup Z). \qquad (b)$$

Obě (neostré) nerovniny (a) a (b) konečně za pomoci zásady ztotožňování zaručují distributivní zákon (axiom) 6′:

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

pro množinové okruhy, c. b. d. (Ověření duálního zákona (axiom 6″) přenechávám čtenáři.) Poznamenejme, že v před-

*) Čtenář sám snadno nahlédne, že množinová inkluse (viz. pozn. 35) je svazovým polouspořádáním v každém množinovém okruhu.

chozím důkazu jsme úmyslně odvodili nerovninu (b) nezávisle na předpokladu, že jde o množinové spojování a protínání, jen ze základních axiomů. Platí tedy tato nerovnina nejen v množinových okruzích, nýbrž v každém svazu vůbec.) Kdybychom se omezili na možinové okruhy, dokázali bychom (v tomto případě téměř zřejmou) nerovninu (b) kratčeji, což doporučuji čtenáři jako snadné cvičení.

Zajímavá a důležitá je tu obrácená souvislost: *Když jsou v libovolném svazu splněny oba distributivní zákony* 6′ *a* 6″, *potom lze takový svaz, jak se říká, representovat množinově.* To znamená, že lze vždy udat *množinový okruh, který je s daným distributivním svazem isomorfní.* Tuto větu[39] o množinové representaci distributivních svazů zde nebudeme dokazovat. Její důkaz není sice obtížný, ale vyžaduje některých pojmů z theorie množin, jež se vymykají z rámce této knížky.

Jsou tedy (množinové okruhy pomocí axiomů 1′ až 4″, 6′ a 6″ *plně abstraktně charakterisovány.*

Distributivními zákony 6′, 6″ však nejsou ještě vyčerpány vlastnosti těch svazů, jako je na př. svaz B_n, které obsahují *veškery části* (podmnožiny) dané množiny. V takových svazech máme ještě další typický axiom, t. zv. axiom komplementu (doplňku).

7. *Ke každému prvku* x (na př. ve svazu B_n) *existuje* (*alespoň jeden*) *prvek* x', *t. zv. doplněk prvku* x, *tak, že platí*:

$$x \cup x' = j, \quad x \cap x' = n$$

(kde j je jednotkový, n je nulový prvek daného svazu).

(Tímto x' k dané části (množině) x je zřejmě souhrn (množina) všech těch uvažovaných předmětů, které nejsou obsaženy v x. Tak na př. ve svazu B_3 všech částí množiny o 3 předmětech a, b, c

$$\text{pro } x = (a, b) \text{ je } x' = (c),$$

pro $x = (b)$ je $x' = (a, c)$ a pod. (Jednotka svazu B_3 je $j = (a, b, c)$, nula svazu B_3, $n = \emptyset$ (prázdná část)).

[39] Čtenář si připomene obdobnou větu z theorie grup (str. 50).

Svazu, který splňuje — kromě základních axiomů 1′ až 5″ — ještě axiom 7 (axiom doplňku) říkáme komplementární svaz.

K samotnému axiomu 7 je třeba poznamenat toto:

Předně, splnění tohoto axiomu žádá již implicitně přítomnost jak jednotkového, tak i nulového prvku ve svazu (axiom 5′, 5″). Tak na př. svaz všech konečných souborů (množin) přirozených čísel, t. j. množinový okruh z př. 4, je sice distributivní, ale nikoli komplementární, protože, ač má nulový, nemá jednotkový prvek. (Tímto jednotkovým prvkem by musela být množina všech přirozených čísel, ale ta je nekonečná). Naproti tomu důležité svazy geometrického spojování a protínání jsou komplementární, ale nikoli distributivní (splňujíce místo axiomů distributivity jistý slabší axiom, t. zv. *axiom modularity*, viz 1,9).

Za druhé, axiom 7 *nežádá jednoznačnost* doplňku: Nikde *není řečeno*, že by doplněk musel být k danému prvku komplementárního svazu *jen jeden*, a skutečně také na př. ve svazech geometrického spojování a protínání není dokonce nikdy jen jeden — až na dvě výjimky: Doplňkem nulového prvku může být vždy jen jednotkový prvek a doplňkem jednotkového prvku může být jen nulový prvek. (Toto pravidlo o jednoznačnosti doplňku jednotky a nuly platí obecně v každém komplementárním svazu. Čtenář si je dokáže jako snadné cvičení 2.) Dokážeme si však co nevidět, že v případě, že jde o distributivní svaz, pak je již (dle axiomů 6′ a 6″) jednoznačnost doplňku ke každému prvku zaručena.

Za třetí, axiomem 7 se zdá porušena duálně souměrná stavba axiomatiky theorie svazů, neboť kde je axiom duální k axiomu 7? Avšak princip duality platí nadále, neboť axiom 7 je duální sám k sobě, jak se pouhým pohledem čtenář přesvědčí. (K jednotce je duální nula, k nule jednotka svazu.)

Výčtem axiomů 1′ až 7 jsme dosáhli uzavřeného a důležitého systému axiomů. (Tato uzavřenost má dokonce doslov-

ný význam; dá se totiž dokázat, že připojení dalšího axiomu, který by měl tvar identity a nebyl důsledkem axiomů právě napsaných, by již vedlo k logickému rozporu.) Svaz, který splňuje všechny dosud vytčené axiomy 1′ až 7 (tedy celkem 13 axiomů) se nazývá distributivním a komplementárním svazem, čili krátce známým nám již názvem Booleova algebra. Příklady Booleových algeber již známe: Jsou to množinové okruhy *všech* částí nějaké dané množiny (konečné nebo i nekonečné); existují však četné jiné příklady.

Theorie Booleových algeber má aplikace v těchto matematických disciplinách: Theorie pravděpodobnosti a statistika, theorie míry a integrálu, obecná topologie, matematická logika, theorie množin. Praktické aplikace mají Booleovy algebry v matematické statistice, v elektrických sítích a v počítacích strojích.

Z theorie Booleových algeber můžeme zde podat ovšem jen malou část. Naším hlavním cílem je věta o množinové representaci Booleových algeber (ovšem jen v konečném případě) — a její užití. Ukážeme si totiž, že ať se dojde ke konečné Booleově algebře jakkoli, vždy lze k ní najít isomorfní algebru všech částí jisté konečné množiny; jsou tedy dosud nám známé příklady *konečných* Booleových algeber typickými příklady. Podstatně složitější jsou poměry v nekonečných Booleových algebrách — a zvláště složité jsou v Booleových algebrách, jakých je potřeba v theorii pravděpodobnosti, kde se totiž dá spojovat (a protínat) nejen konečně, ale i nekonečně mnoho prvků. Těmito aplikacemi theorie Booleových algeber se však nemůžeme zde zabývat. Omezíme naše úsilí na to, abychom si objasnili podstatu aplikace konečných Booleových algeber v *elektrotechnice* a v *matematické logice*.

Cvičení k 2,4.

1. Dokažte (postupem duálním k postupu v textu) platnost duálního distributivního axiomu v množinových okruzích.

2. Dokažte, že k jednotkovému prvku v libovolném svazu může

být doplňkem jen nulový prvek a k nulovému prvku jen jednotkový prvek — je-li splněn axiom 7 doplňku.

3. Dokažte, že rovnost $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ je v každém svazu vždy splněna, je-li některý z prvků (a, b, c) nulou svazu. Totéž pro jednotku svazu na místě nuly. Totéž pro rovnost duální $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

4.*Dokažte, že svaz geometrického spojování a protínání bodů, přímek a rovin (k nimž přidána prázdná část prostoru = nulový prvek svazu) a celý prostor = jednotkový prvek svazu) není distributivní.

(Návod: Zvolte a, b, c vhodně jako bod, přímku, rovinu.)

5.*Najděte, které ze svazů na obr. 16, 17, 18, 19 jsou distributivní. Které z nich splňují axiom doplňku? Které obojí?

6.*Dokažte, že svaz je distributivní, když a jen když neobsahuje podsvaz tvaru IV ani podsvaz tvaru V z obr. 19.

(Ukažte, že existence takových podsvazů by porušovala distributivní zákon — a obráceně, že tři prvky a, b, c porušující distributivní zákon, by vytvořily podsvaz typu IV nebo V z obr. 19.)

7.* Dokažte, že svaz všech kladných celistvých dělitelů libovolného celého čísla $N \geqq 1$ (ve smyslu dělitelnosti jakožto částečného uspořádání) je konečný distributivní. Kolik prvků má tento svaz? Co je nulou a co jednotkou svazu?

8. Dokažte, že svaz všech racionálních dělitelů celého čísla N, které jsou celistvými násobky čísla $\frac{1}{N}$ (ve smyslu cvičení 4 k 2,3) je distributivní konečný svaz o jednotce svazu rovné číslu N a nule svazu rovné číslu $\frac{1}{N}$.

2,5. THEORIE (KONEČNÝCH) BOOLEOVÝCH ALGEBER.

Odvoďme si nejprve několik jednoduchých a potřebných důsledků z axiomů pro distributivní a komplementární svazy (Booleovy algebry).

1. *V distributivním svazu může existovat* (ve smyslu axiomu 7) *nejvýše jeden doplněk k danému prvku.* — Neboť vskutku, nechť k prvku x daného distributivního svazu — rozumí se svazu s nulou n a s jednotkou j — máme dva doplňky, x' a x^+. Pak je tedy (dle axiomu 7)

$$x \cup x' = j,\ x \cap x' = n,\ x \cup x^+ = j,\ x \cap x^+ = n.$$

Protněme první z napsaných rovností na obou stranách prvkem x^+. Pomocí axiomů 6′ a 5′ dostáváme

$$x^+ = (x \cup x') \cap x^+ = (x \cap x^+) \cup (x' \cap x^+) = \\ = n \cup (x' \cap x^+) = x' \cap x^+,$$

tedy

$$x^+ = x' \cap x^+.$$

Záměnou x' za x^+ dostáváme právě tak $x' \cap x^+ = x'$, když jsme užili ještě cestou axiomu komutativity 3″. Tedy musí být $x' = x^+$; doplněk je jen jeden.

2. *V každé Booleově algebře platí užitečná početní t. zv. pravidla De Morganova*:

$$(x \cup y)' = x' \cap y'$$

(slovy: Doplněk spojení je průnikem doplňků).

$$(x \cap y)' = x' \cup y'$$

— obojí pro libovolné dva prvky x, y (slovy: Doplněk průniku je spojením doplňků).

Dokažme třebas jen druhé z obou pravidel. První se dokáže duálním způsobem, což si opět čtenář provede laskavě sám jako cvičení.

Máme dokázat, že prvek $x' \cup y'$ splňuje požadavky na doplněk k prvku $x \cap y$. Za pomocí axiomů 2′, 5′ a 6′ máme vskutku

$$(x \cap y) \cup (x' \cup y') = [(x \cap y) \cup x'] \cup y' = \\ = [(x \cup x') \cap (x' \cup y)] \cup y' = (x' \cup y) \cup y' = x' \cup (y \cup y') = \\ = x' \cup j = j$$

to jest (poněvadž ostrá nerovnina je zřejmě vyloučena)

$$(x \cap y) \cup (x' \cup y') = j.$$

Stejně je i

$$(x \cap y) \cap (x' \cup y') = x \cap [y \cap (x' \cup y')] = \\ = x \cap [(x' \cap y') \cup (y \cap y')] = x \cap (x' \cap y') = \\ = (x \cap x') \cap y' = n \cap y' = n$$

3. *Pravidlo o převrácení polouspořádání doplňováním*: Když je $x \subseteq y$, pak je $y' \subseteq x'$.

$x \subseteq y$ značí totiž $x \cup y = y$, tedy i $y' = (x \cup y)'$ (dle jednoznačnosti doplňku). Dle prvního De Morganova pravidla je však $y' = x' \cap y'$, což značí $y' \subseteq x'$.

4. *Pravidlo o dvojím doplňku*:
Pro každý prvek x platí

$$(x')' = x.$$

Neboť ve smyslu axiomu 7 prvek x splňuje požadavky toho, aby byl doplňkem k prvku x' — jestliže ovšem ještě přihlédneme k axiomům komutativity 3′, 3″.

5. *Pravidlo o převádění polouspořádání na anulovanou rovnost*: Je $x \subseteq y$ tehdy a jen tehdy, když $x \cap y' = n$.

Jednak totiž protnutím nerovniny $x \subseteq y$ na obou stranách prvkem y' máme $x \cap y' \subseteq y \cap y' = n$, jednak spojením obou stran rovnosti $x \cap y' = n$ s prvkem y máme (užitím axiomu distributivity)

$$(x \cup y) \cap (y \cup y') = x \cup y = y,$$

což značí

$$x \subseteq y.$$

A nyní velmi potřebná obecná definice:

Říkáme, že prvek p svazu, (po případě Booleovy algebry) B je atomem (též někdy sousedem nuly), když jediným prvkem z z B splňujícím nerovnost $z \subset p$ je nula $n = z$ svazu (algebry) B.

Věta (o množinové representaci konečné Booleovy algebry):

Každá konečná Booleova algebra B je isomorfní s Booleovou algebrou (t. j. s množinovým okruhem) B_N *všech skupin utvořených z vhodného konečného počtu N předmětů.*

Důsledek věty: *Každá Booleova konečná algebra má 2^N prvků (při vhodném N přirozeném). Všechny Booleovy algebry o stejném konečném počtu prvků jsou navzájem isomorfní.*

Důkaz věty:

Nejprve dokažme, že každý od nuly různý prvek a dané konečné Booleovy algebry B obsahuje alespoň jeden atom p, t. j. je

$$p \subseteq a.$$

Najdeme za tím účelem — je-li to možno — k prvku $a \neq n$ prvek $a_1 \neq n$ tak, že je $a_1 \subset a$. Není-li to možno, pak ovšem musí být podle definice prvek a sám atomem, $a = p$, čímž jsme žádaného docílili. — V prvním případě učiňme dále totéž s prvkem a_1 místo původního prvku a. Opět buďto je $a_1 = p$ je sám atom, pak $p \subset a$ a jsme hotovi, anebo možno nalézt další prvek a_2 tak, že je $n \subset a_2 \subset a_1 \subset a$. Tak pokračujíce můžeme učinit nanejvýše tolik kroků a dospět k t. zv. klesajícímu řetězci

$$a_k \subset a_{k-1} \subset \ldots \subset a_1 \subset a$$

takové délky, kolik je prvků algebry B (ve skutečnosti, je ovšem nejvyšší možná délka klesajícího řetězce mnohem menší než počet prvků naší algebry). Zřejmě poslední člen a_k takového klesajícího řetězce, který se již nedá prodloužit, je hledaným atomem, $p = a_k \subset a$.

Utvořme nyní spojení $p_1 \cup p_2 \cup \ldots \cup p_r = b$ všech vzájemně různých atomů, které jsou obsaženy v daném prvku $a \neq n$, $p_i \subseteq a$ $(i = 1, 2, \ldots, r)$. (Je jasné, že těchto atomů je konečný počet r, protože všech prvků algebry je konečně mnoho.)

Tvrdím, že

$$b = a.$$

Za účelem tohoto důkazu si pišme

$$a = a \cap j = a \cap (b \cup b') = (a \cap b) \cup (a \cap b') = \\ = b \cup (a \cap b')$$

(protože je ovšem $b \subseteq a$, takže $a \cap b = b$). Kdyby bylo $b \neq a$, pak by z právě napsaného plynulo $a \cap b' \neq n$. Z druhé strany je ovšem $a \cap b' \subseteq a$. Tedy bychom podle svrchu řeče-

ného mohli nalézt jakýsi atom p, splňující $p \subseteq a \cap b' \subseteq a$. Pak by platilo

$$b \cap p = (p_1 \cup p_2 \cup \ldots \cup p_r) \cap p \subseteq b \cap (a \cap b') = n,$$

čili — užitím distributivního zákona — by bylo

$$(p_1 \cap p) \cup (p_2 \cap p) \cup \ldots \cup (p_r \cap p) = n.$$

To ovšem znamená, že každý člen napsaného spojení by byl n, čili že je $p \neq p_i$ pro $i = 1,2, \ldots r$, ačkoli p je jeden z atomů obsažených v a. — Ježto tedy by možnost ostré nerovniny ve vztahu $b = p_1 \cup p_2 \cup \ldots \cup p_r \subseteq a$ vedla k nemožnému důsledku, musí ve skutečnosti nastat rovnost $b = a$.

Tvrdím dále, že vyjádření libovolného prvku $a \neq n$ naší algebry spojením všech atomů v něm obsažených je jednoznačné, t. j. že žádné jiné atomy nedávají svým spojením prvek a.

Že každý atom, vystupující v libovolném spojovém vyjádření prvku a, je obsažen v a — je jasné. Mohlo by se tedy nanejvýš snad stát, že by již i vlastní část atomů, obsažených v a stačila k vyjádření a jejich spojením. V takovém případě bychom však jistě vynecháním některého atomu (a budiž to při vhodném označení zrovna atom p_r) z napsaného spojového vyjádření prvku a ještě obdrželi prvek a, $a = p_1 \cup \cup p_2 \cup \ldots \cup p_{r-1}$. Avšak protněme tuto rovnost na obou stranách atomem p_r. Dostáváme — za pomoci distributivního zákona

$$p_r = a \cap p_r = (p_1 \cap p_r) \cup (p_2 \cap p_r) \cup \ldots \cup (p_{r-1} \cap p_r)$$

následkem $p_r \subseteq a$. Avšak na druhé straně je jasné, že jednotliví členové napsaného spojení, prvky $p_i \cap p_r$ (pro $i = 1, 2, \ldots, r - 1$), jsou podle definice atomu vesměs rovny nule n, tedy i jejich spojení $= n$, což dává spor. To znamená, že žádný z atomů obsažených v prvku $a \neq n$ nelze postrádat, chceme-li jejich spojením dostat a.

Utvořme nyní soubor (množinu) všech atomů naší Booleovy algebry, jichž budiž N. Utvořme všechny skupiny

atomů (včetně skupiny prázdné a plné). Přiřaďme každému prvku $a \neq n$ naší algebry podle právě řečeného skupinu atomů, jež jsou v něm obsaženy. Pak každá skupina atomů vzájemně jednoznačně odpovídá prvku naší algebry. Nule n naší algebry přiřadíme pochopitelně prázdnou skupinu atomů. Přiřazení můžeme vyznačit takto: $a \longleftrightarrow (p_1, p_2, \ldots, p_r)$, jestliže $a = p_1 \cup p_2 \cup \ldots \cup p_r$, kde ovšem $0 \leqq r \leqq N$ ($r = 0$ pro $a = n$).

Jde již jen o to dokázat, že jestliže ještě prvku b je takto přiřazena skupina atomů $(q_1, q_2, \ldots, q_s)$, pak: Spojení $a \cup b$ je tímto způsobem přiřazeno sjednocení obou skupin atomů, průseku $a \cap b$ je přiřazen průnik obou skupin atomů a doplňku a' je přiřazena skupina atomů, neobsažených v a; neboť právě toho si žádá isomorfismus, o nějž ve větě jde.

Skutečně, patrně je

$$a \cup b = p_1 \cup p_2 \cup \ldots \cup p_r \cup q_1 \cup q_2 \cup \ldots \cup q_s,$$

při čemž ovšem některé atomy se v tomto spojení mohou vyskytovat dvakráte. Podržíme-li z takových dvakráte se vyskytujících atomů vždy jen jeden ve spojení, obdrželi jsme jednoznačné vyjádření prvku $a \cup b$ jakožto spojení vzájemně různých atomů. Avšak soubor těchto atomů je nyní zřejmě sjednocením skupiny $(p_1, \ldots, p_r)$ se skupinou $(q_1 \ldots q_s)$.

Podobně máme pomocí axiomů distributivity:

$$a \cap b = (p_1 \cup \ldots \cup p_r) \cap (q_1 \cup \ldots \cup q_s) =$$
$$= (p_1 \cap q_1) \cup (p_1 \cap q_2) \cup \ldots \cup (p_1 \cap q_s) \cup \ldots \cup (p_r \cap q_s) =$$

= spojení všech průniků každého atomu, obsaženého v a — s každým atomem, obsaženým v b. Z definice atomu však plyne, že je $p_i \cap q_k \neq n$ (pro $i = 1, 2, \ldots, r$, $k = 1, 2, \ldots, s$) tehdy a jen tehdy, když $p_i = q_k$, kdy ovšem $p_i \cap q_k = p_i = q_k$ je atom, obsažený jak v a tak i v b. Tím však je řečeno, že v průseku obou prvků a, b jsou právě a jen obsaženy ty atomy, jež jsou současně obsaženy v obou, čili jež tvoří do-

hromady průnik obou skupin atomů, přiřazených jednomu a druhému prvku.

Konečně pokud jde o doplněk: Je-li $a = p_1 \cup \ldots \cup p_r$, pak nechť všechny ostatní atomy (navzájem různé a různé od všech p_i $(i = 1, 2, \ldots, r)$ jsou $q_1, q_2, \ldots, q_s$. (Pak ovšem $s = N - r$.) Utvořme jejich spojení, prvek $q_1 \cup \ldots \cup q_s$. Čtenář se již sám přesvědčí, že tento prvek má vlastnosti, jež jsou požadovány od doplňku k prvku a, čímž je důkaz naší věty dokončen.

Vidíme tedy, že dle věty 1 lze studium konečných Booleových algeber převést na studium systémů všech částí konečných množin.

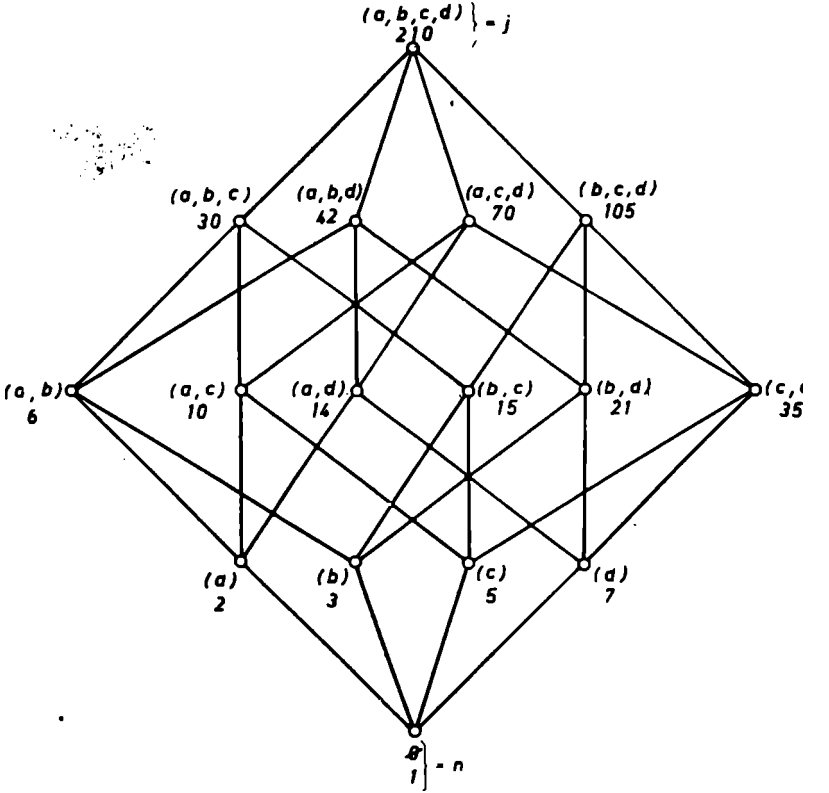
Jak již bylo řečeno, v nekonečných Booleových algebrách nejsou poměry zdaleka tak jednoduché. Každá i nekonečná Booleova algebra se dá sice isomorfně representovat jistým množinovým okruhem, který však jen zcela výjimečně může být systémem všech částí vhodné (nekonečné) množiny. Jednoduchý příklad Booleovy algebry podstatně různé od systému všech částí množiny nám to osvětlí. Mysleme si systém všech částí (podmnožin) množiny všech přirozených čísel 1, 2, 3, ... Vyberme si však z tohoto systému jen: *Podmnožiny konečné a jejich doplňky*, t. j. nekonečné množiny s konečnými doplňky. (Tak na př. množina (2, 4) a množina (1, 3, 5, 6, 7, ...) budou patřit mezi takto vybrané množiny přirozených čísel.) Tvrdím, že tento systém množin tvoří nejen množinový okruh, ale právě Booleovu algebru. Skutečně, sjednocení a ovšem i průnik dvou konečných množin přirozených čísel je zase konečná množina. Rovněž průnik konečné množiny s nekonečnou množinou (která má konečný doplněk, ale nejen s takovou, nýbrž vůbec s každou) je konečný. Sjednocení konečné množiny s nekonečnou, která má konečný doplněk, je ovšem nekonečná množina, která má tím spíše konečný doplněk. Sjednocení dvou množin nekonečných o konečných doplňcích je rovněž tím spíše nekonečná množina, která má konečný doplněk. A konečně i průnik dvou nekonečných množin o vesměs konečných doplňcích je opět množina nekonečná o konečném doplňku, protože tento doplněk průniku je jako dle De Morganova pravidla, jak čtenář snadno nahlédne, roven sjednocení doplňků, což jsou však dle předpokladu konečné množiny. Co se týče doplňků, je nyní již jasno, že jsou v pořádku.

Avšak je nejen zřejmo, že takto sestrojená nekonečná Booleova algebra neobsahuje všechny části množiny přirozených čísel jako prvky (na př. není v ní množina všech lichých čísel), nýbrž snadno se dá ukázat, že ani nemůže být s žádným systémem všech částí nějaké

množiny isomorfní. (Čtenář, který zná Pospíšilovu knížku o nekonečnu v matematice, resp. který ví, co jsou to nespočetné mohutnosti množin, ví již odtud, proč nemůže být naše spočetná algebra isomorfní s algebrou všech částí nějaké množiny.)

Dříve, než se obrátíme k zběžnému naznačení aplikací (konečných) Booleových algeber, pozdržme se chvilku u geometrického (grafického) znázornění konečných Booleových algeber. Tvrdím, co bylo již na obrázcích naznačeno: Že totiž za geometrické (grafické) znázornění Booleovy algebry lze vždy pokládat krychli, postavenou na jeden vrchol, ovšem v prostoru o příslušné dimensi N, jestliže algebra má (dle věty 1) 2^N prvků. (Pro $N = 1, 2, 3$ to již známe z obr. 16, 18 I a 14.) Dle věty 1 lze totiž každou konečnou Booleovu algebru v podstatě pokládat za systém všech podmnožin jakékoli konečné množiny o N prvcích. Myslemе si N navzájem orientovaných os (euklidovského) N-rozměrného prostoru. Na kladnou polovičku každé z nich nanesme od počátku délku 1. Pak takto získaných N bodů (o souřadnicích vždy až na jednu (i-tou) vesměs rovných nule (i probíhá $1, \ldots, N$)), nechť tvoří naši konečnou množinu. Z ní nyní máme utvořit všechny části, t. j. všechny skupiny základních (nejprostších číselných N-tic, kde však jsou v každé N-tici samé nuly, a jen na jednom místě (i-tém) je 1. Každou takovou skupinu N-tic lze však považovat za jedinou N-tici, která vykazuje 1 na těch a jen těch místech, kde byla 1 v některé ze základních N-tic z dané skupiny (na ostatních místech má výsledná N-tice nuly). To však není nic jiného než souřadnice jednotlivých rohů N-rozměrné krychle o hraně 1. Snadno se pak dokáže, že spojení dvou prvků dané konečné Booleovy algebry se nyní geometricky representuje takto: Ke dvěma prvkům, t. j. teď rohům naší N-rozměrné krychle, najdeme jejich *spojení* jakožto roh, který je *co nejblíže počátku* (jenž odpovídá nule algebry), z těch rohů, do nichž se lze dostat z jednoho i z druhého daného rohu po hranách krychle za *neustálého vzdalování se od počátku* souřadnic. Podobně přechází vyhledávání *průseku* dvou prvků algebry, t. zn. dvou rohů naší krychle, ve vyhledávání od počátku co nejvzdálenějšího rohu krychle, do něhož se lze dostat z obou daných vrcholků po hranách krychle, za *neustálého blížení se k počátku*. Konečně není těžké nahlédnout, že doplněk k danému vrcholku naší krychle jakožto prvku Booleovy algebry, je protilehlý vrcholek, t. j. ten, do něhož vede přímá spojnice daného vrcholku se středem krychle (4-rozměrná krychle, představující Booleovu algebru o $2^4 = 16$ prvcích, je na obr. 21).

A nyní se obraťme k naznačení některých aplikací konečných Booleových algeber.



Obr. 21.

Cvičení k 2,5.

1. Dokažte první De Morganovo pravidlo (identitu) pro Booleovy algebry.

2. Dokažte, že atom je právě takový prvek q v Booleově algebře, pro nějž platí, když je $x \cup y = q$, pak buďto $x = q$, nebo $y = q$.

3. Dokažte, že atom je v Booleově algebře právě takový prvek q, pro který platí, když je $x \supset q'$, pak je již $x = j$ (jednotka algebry).

4. Dokažte, že distributivní svaz všech celistvých dělitelů celého čísla $N > 1$ (ve smyslu svazového polouspořádání dle vztahu dělitelnosti) je Booleova algebra tehdy a jen tehdy, když číslo N nemá čtvercových dělitelů. (Viz cvičení 6 k 2,4.)

2,6. „RACIONÁLNÍ FUNKCE" NA BOOLEOVĚ ALGEBŘE (BOOLEOVSKÉ FUNKCE). ÚPLNÉ NORMÁLNÍ FORMY.

Vyjděme opět z analogie s čísly.

Čtenář si vzpomene, že t. zv. racionální funkce ve školské algebře jsou zhruba řečeno takové funkce (mající za hodnoty t. zv. argumentu vždy jedno nebo i více čísel a za hodnoty funkce vždy jedno číslo), kde hodnota funkce se dá vypočítat z hodnot argumentu dle vhodného početního předpisu, skládajícího se z kombinovaného sečítání, odčítání, násobení a (pokud dělitel není nula) dělení.

(Příklady takových racionálních početních předpisů, jež čtenář dobře zná, jsou

$$f(x) = \frac{x^2 - 1}{x},\ g(x, y) = \frac{x^2 + 2xy + 3}{x + y},$$

$$h(x, y, z) = \frac{1 + x^2}{3{,}2\,.\,y} + y + \frac{2{,}5}{z},\ \text{atp.}).$$

V takovém početním předpisu pro racionální funkci vystupují, jak známo, jednak určitá pevná čísla, t. zv. konstanty a jednak t. zv. nezávisle proměnné (neurčité), a to v konečném (ale zásadně neomezeném) počtu m, na př. jsou to $x, y, z, \ldots$ anebo jsou to $x_1, x_2, \ldots$ Provedení předpisu spočívá v tom, že při daném argumentu, t. j. uspořádané skupině čísel $a_1, a_2, \ldots, a_m$ se prostě dosadí za odpovídající nezávisle proměnné jim odpovídající čísla, t. zn. řekněme číslo a_1 za proměnnou x_1, a_2 za x_2 atd. až posléze a_m za x_m, a takto naznačené početní úkony se provedou (s výjimkou neproveditelného dělení nulou, pokud se vyskytne). Výsledek je hodno-

ta dané racionální funkce pro daný argument (pro dané hodnoty nezávisle proměnných). (Na př.

$$f(1) = \frac{1^3 - 1}{1} = 0,\ g(1, 2) = \frac{1^2 + 2 \,.\, 1 \,.\, 2 + 3}{1 + 2} = \frac{8}{3} \text{ atp.})$$

Při tom je třeba si povšimnout a zdůraznit, že (racionální) *funkce sama je něco jiného, než příslušný početní předpis*; jedna a táž racionální funkce může být dána různými početními předpisy (postupy), které však dávají při tomtéž argumentu týž výsledek. Na př.

$$f(x) = \frac{x^2 - 1}{x} = (x - 1)(x + 1)\ \frac{1}{x},\ g(x, y) =$$

$$= \frac{x^2 + 2xy + 3}{x + y} = x + y + \frac{3 - y^2}{x + y}, \text{ atp.})$$

Čtenář ví dále, že sečítat, odčítat, násobit a dělit (pokud bychom nechtěli dělit nulou) lze nejen čísla, ale i samotné racionální funkce.

Při tom definujeme přirozeně jako součet $h(x)$ dvou racionálních funkcí, $f(x)$ a $g(x)$ tu racionální funkci, která číslu x přiřazuje součet obou funkčních hodnot, $f(x) + g(x) = h(x)$. Podobně definujeme rozdíl, součin a (pokud bychom se nedopouštěli dělení nulou) i podíl dvou racionálních funkcí jakožto racionální funkci. Početní předpis, kterým je vlastně takto součet, rozdíl, součin a podíl dvou racionálních funkcí přímo definován, hledíme ovšem vhodnou úpravou zpravidla změnit (zjednodušit). Tak na př. je-li

$$f(x) = \frac{x^2 - 1}{x},\ g(x) = \frac{1}{x},$$

pak

$$h(x) = f(x) + g(x) = \frac{x^2 - 1}{x} + \frac{1}{x} = x$$

ovšem jen pro $x \neq 0$.

Avšak je zapotřebí sečítat, odečítat, násobit a dělit i racionální funkce, které se neshodují ve všech svých nezávisle proměnných. Pak součet, rozdíl, součin, podíl takových dvou racionálních funkcí je i v tomto obecnějším případě definován stejně — výsledkem je ovšem racionální funkce obecně všech nezávisle proměnných, která se vyskytují v jedné, nebo v druhé z daných funkcí. (Tak na př. pišme

$$f(x) + g(y) = \frac{x^2 - 1}{x} + \frac{1}{y} = \frac{x^2 + xy - 1}{xy} = u(x, y),$$

$$f(x) + g(x, y) = \frac{x^2 - 1}{x} + \frac{x^2 + 2xy + 3}{x + y} =$$

$$= \frac{2x^3 + 3x^2y + 2x - y}{x^2 + xy} = v(x, y), \text{ atp.})$$

A nyní: V Booleově algebře nalézáme úplnou obdobu racionálních funkcí. Prohlásíme nyní za „racionální funkci" na dané Booleově algebře B čili kratčeji za booleovskou funkci takové přiřazení f vždy určitého jediného prvku $f(x_1, x_2, \ldots, x_m)$ dané Booleovy algebry B k libovolně zvolené m-tici prvků $x_1, x_2, \ldots, x_m$ z této algebry, které lze uskutečnit vhodným (pro všechny hodnoty proměnných týmž) „početním" booleovským předpisem (hodnota funkce se dá „vypočítat"). Při tom ovšem se tímto *„početním" booleovským předpisem rozumí opakování a kombinování základních úkonů Booleovy algebry* B, t. j. určitý sled *spojování, protínání a doplňování*, prováděného na „proměnných" prvcích $x_1, x_2, x_3, \ldots, x_m$ (jež si lze libovolně volit), jakož i na jistých „konstantách" (které jsou neměnnými prvky vystupujícími v řečeném početním booleovském předpisu). Nejjednodušší booleovské funkce, dané přímo jediným základním úkonem, jsou vyznačeny v tab. 2. — Je-li a pevný prvek („konstanta") dané Booleovy algebry B, pak je ještě dosti jednoduchá funkce dána třeba předpisem: $f(x) = (x \cup a) \cap x'$. (Je to booleovská funkce o jedné nezávisle proměnné x.) Je-li b konstanta, pak je předpisem

TABULKY NEJJEDNODUŠŠÍCH DVOJHODNOTOVÝCH BOOLEOVSKÝCH FUNKCÍ NA BOOLEOVĚ ALGEBŘE (0,1).

x	x'
1	0
0	1

x_1	x_2	$x_1 \cup x_2$	$x_1 \cap x_2$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

Tab. 2.

$$g(x, y) = [(x \cup y) \cap (a \cup x) \cap (b \cup y)] \cap x'$$

dána booleovská funkce g o dvou nezávisle proměnných x a y, atp.

(Dosaďme na př. za $x = n$ (nulu algebry). V prvém příkladě funkce $f(x)$ „vypočteme" příslušnou hodnotu funkce takto:

$$f(n) = (n \cup a) \cap n' = a \cap j = a$$

Podobně, dosaďme do druhého předpisu pro funkci g třeba $x = n$, $y = j$ (jednotka algebry). Dostáváme

$$g(n, j) = [(n \cup j) \cap (a \cup n) \cap (b \cup j)] \cap n' = \\ = (j \cup a \cup j) \cap j = j,$$

jakožto hodnotu funkce g pro hodnotu (n, j) argumentu (čili pro hodnotu n první a hodnotu j druhé nezávisle proměnné).)

V tab. 3 je tabelována obecnější funkce

$$f(x_1, x_2, x_3) = (x_1 \cup x_2) \cap x_3'$$

o třech proměnných. Podobně, jako u číselných funkcí, i Booleovské funkce můžeme udat tabulkou.

Opět ovšem musíme zdůraznit, že — jako při obyčejných racionálních funkcích — i zde jedna a táž booleovská funkce (čili jedna a táž tabulka, může být dána různými početními booleovskými předpisy. Tak na př. lze psát právě tak dobře v prvním příkladě $f(x) = x' \cap a$, v druhém příkladě

$$g(x, y) = (x \cup y) \cap (a \cap x') \cap (b \cup y),$$

jak se čtenář sám snadno přesvědčí.

A opět podobně, jako jsme sečítali, odčítali a násobili a dělili samotné racionální funkce, můžeme *spojovat a protínat a doplňovat* samotné booleovské funkce, čili můžeme *utvořit Booleovu algebru* všech booleovských funkcí na dané Booleově algebře B.

Při tom budeme patrně spojením $[f \cup g](\ldots)$ dvou takových booleovských funkcí $f(\ldots)$ a $g(\ldots)$ na B rozumět booleovskou funkci, která uspořádané m-tici hodnot nezávisle proměnných, které se vyskytují v jedné nebo v druhé funkci, přiřazuje jako hodnotu spojení obou příslušných hodnot funkce $f(\ldots)$ a funkce $g(\ldots)$. (Tak na př. je-li

$$f(x) = x \cap a, \; g(x, y) = x' \cup y \cup b;$$

pak

$$[f \cup g](x, y) = (x \cap a) \cup (x' \cup y \cup b) = \\ = x' \cup a \cup y \cup b)$$

jak se čtenář sám snadno přesvědčí.)

Stejně budeme definovat průsek dvou Booleových funkcí $f \cap g(\ldots)$ jakožto funkci, jejíž hodnoty jsou dány průsekem hodnot obou funkcí. (Na př. shora

$$[f \cap g](x, y) = (x \cap a) \cap (x' \cup y \cup b) = \\ = [(x \cap y) \cup (x \cap b)] \cap a.$$

Konečně doplňkem $f'(\ldots)$ booleovské funkce $f(\ldots)$ budeme patrně rozumět funkci přiřazující daným hodnotám argumentu doplněk příslušné hodnoty funkce $f(\ldots)$.

Omezme nyní počet nezávisle proměnných číslem m a za algebru B vezměme nějakou konečnou Booleovu algebru, t. j.

dle předchozí věty algebru všech částí konečné množiny řekněme o N prvcích. Dostáváme tedy jistou algebru funkcí. Jde o to, kolik nanejvýše prvků (t. j. booleovských funkcí) obsahuje tato Booleova algebra.

Jelikož algebra B má 2^N prvků, je všech možných m-tic prvků z B, čili všech možných hodnot argumentu právě $(2^N)^m = 2^{mN}$ (což je počet všech m-členných variací s opakováním z 2^N prvků, jak si čtenář ze školy vzpomene). Booleovy funkce o m-nezávisle proměnných můžeme považovat za variace s opakováním. Bude tedy všech booleovských funkcí o m nezávisle proměnných nejvýše (ve skutečnosti právě tolik, kolik je 2^{mN} členných pořadí variací s opakováním z 2^N prvků, t. j. $2^{N2^{mN}}$.

Především je tedy ovšem počet všech Booleových funkcí o m nezávisle proměnných na konečné Booleově algebře konečný. Máme tak příklady konečných Booleových algeber, které nejsou přímo dány jakožto množinové okruhy. Nicméně podle poslední věty jsou i tyto algebry funkcí vždy isomorfní s vhodnou algebrou všech částí jisté konečné množiny.

V dalším se věnujme nejjednoduššímu, ale v aplikacích nejdůležitějšímu případu algebry — označme ji A_m — Booleových funkcí nezávisle proměnných na Booleově algebře $B = (n, j)$ jen o dvou prvcích: Nule n $(= \emptyset$ a jednotce j $(= (a))$. (Zde je $N = 1$, B je algebra všech částí množiny (a) o jediném předmětu.) Dle předchozí poznámky je počet prvků v algebře A_m nejvýše 2^{2^m} (uvidíme brzy, že je přesně takový). Jde o to, abychom získali bližší náhled na algebru A_m.

Vyjděme opět z analogie s racionálními funkcemi. Jak čtenář dobře ví, při úpravě početního předpisu pro obyčejnou racionální funkci (číselnou) si počínáme zpravidla tak, že odstraníme případné složené zlomky, pronásobíme výrazy v závorkách a uvedeme vše na společný jmenovatel. Tak se předpis pro racionální funkcí objeví ve tvaru zlomku, kde v čitateli i v jmenovateli je mnohočlen v nezávisle proměnných, při čemž ještě uspořádáváme obvykle i jednotlivé členy v mnohočlenech podle klesajících mocnitelů u proměnné; pokud je více různých nezávisle proměnných, určíme si zpravidla předem jejich pořadí (na př. $x_1, x_2, \ldots$, nebo dle

abecedy $x, y, z, \ldots$ pokud tato stačí), a pořadí členů v mnohočlenu o více proměnných určujeme t. zv. lexikografickým způsobem. Dáváme totiž přednost členům s vyšším stupněm (t. j. součtem mocnitelů) a při stejném stupni uspořádáváme členy tak, jako by to byla hesla ve slovníku. Tak bychom na př. upravili

$$h(x, y) = \frac{x^2 - 1}{x} + \frac{x^2 + 2xy + 3}{x + y} = \frac{2x^3 + 3x^2y + 2x - y}{x^2 + xy}.$$

Taková standardní úprava nám představuje jakousi normální formu početních předpisů pro racionální funkci. Ovšem že toto není jediná možná standardní úprava — a není ani vždy nejvhodnější. (Tak na př. někdy je lepší provést naznačené částečné dělení (se zbytkem) a psát třeba

$$h(x, y) = 2x + \frac{x^2y + 2x - y}{x^2 + xy}.$$

Takové úpravy v typické normální formy máme i pro početní předpisy booleovské (pro booleovské funkce). Z nich jsou nejdůležitější dvě: T. zv. úplná spojová (někdy též disjunkční) normální forma, a t. zv. úplná průseková (či též konjunkční) normální forma, která je k první duální.

Pod úplnou spojovou normální formou v m proměnných $x_1, x_2, \ldots, x_m$ rozumíme spojení několika různých průseků, z nichž každý má m činitelů a tito činitelé jsou buďto samy proměnné x_i anebo jejich doplňky (při čemž udané pořadí proměnných v průsecích zachováváme); nikdy však není v jednom průseku současně proměnná a její doplněk. (Takový průsek by ostatně dal vždy nulu a mohl by se ve spojení vynechat.)

Podobně pod t. zv. úplnou průnikovou (konjunkční) normální formou rozumíme duálně průsek několika spojení, z nichž každé má m činitelů a tito činitelé jsou vesměs buďto samy proměnné, nebo jejich doplňky — při čemž nikdy není v jednom spojení proměnná

i její doplněk (takové spojení by se jakožto činitel průseku vynechalo, jsouc vždy rovno jednotce).

Příklady spojové, čili, jak se též někdy říká, disjunkční normální formy:

$$F(x_1, x_2, \ldots, x_m) = (x_1' \cap x_2' \cap x_3 \cap \ldots \cap x_m) \cup (x_1 \cap x_2' \cap x_3 \cap \ldots \cap x_m),$$

$$G(x_1, \ldots, x_m) = (x_1' \cap x_2' \cap \ldots \cup x_m') \cup (x_1' \cap x_2 \cap \ldots \cap x_m) \cup (x_1 \cap x_2 \cap \ldots \cap x_m).$$

(Příklady na průsekovou normální formu si čtenář snadno dualisací sestrojí sám.)

Půjde nyní o to ukázat, že každý (sobe složitější) početní předpis, udávající booleovskou funkci o m nezávisle proměnných, se dá uvést na úplnou spojovou normální formu. (Jde stále o booleovské funkce, kde nezávisle proměnné nabývají každá jen dvou hodnot, nuly n resp. jednotky j z dvouprvkové algebry (n, j) a kde hodnoty závisle proměnné jsou opět buďto n nebo j.

(Poznamenejme, aby nebylo nedorozumění: Místo o všech uvažovaných booleovských funkcích o m proměnných můžeme právě tak dobře mluvit o všech (booleovských) funkcích o *nejvýše* m nezávisle proměnných. Neboť funkce $f(x_1, \ldots, x_{m-r})$ $(0 \leqq r < m)$, v jejímž početním předpisu vystupují řekněme jen nezávisle proměnné $x_1, \ldots, x_{m-r}$, může být považována za funkci všech m nezávisle proměnných $F(x_1, \ldots, x_m)$, jestliže prostě stanovíme, že při týchž daných hodnotách $x_1, \ldots, x_{m-r}$ jsou hodnoty funkce $F(x_1, \ldots, x_m)$ stále stejné a rovny hodnotě $f(x_1, \ldots, x_{m-r})$, ať jsou hodnoty ostatních proměnných $x_{m-r+1}, \ldots, x_m$ jakékoli.)

Věta. (O úplné spojové normální formě v Booleově algebře funkcí m nezávisle proměnných na algebře (n, j).)

Každá booleovská funkce o m nezávisle proměnných na Booleově algebře $B = (n, j)$ *se dá vyjádřit jedním a jen jedním způsobem v t. zv. úplné spojové normální formě jakožto spojení nejvýše* 2^m *průseků; průsek má m činitelů, jež jsou buď přímo ne-*

závisle proměnné, nebo jejich doplňky (ale ne obojí současně). Všechny tyto booleovské funkce tvoří Booleovu algebru A_m, která má 2^{2^m} prvků a zmíněné význačné průseky (spojované v t. zv. úplné spojové normální formě) jsou její atomy. Algebra A_m je tedy isomorfní s množinovou Booleovou algebrou všech částí libovolné množiny o 2^m prvcích.

Důkaz:

V jakém smyslu naše booleovská funkce o m nezávisle proměnných na algebře (n, j) tvoří Booleovu algebru A_m, už víme.

Vyjdeme z následujícího vyjádření jednotky $j(\ldots)$ algebry A_m (vlastně z funkce, která nabývá vždy hodnoty j):

$$j(\ldots) = (x_1 \cup x_1') \cap (x_2 \cup x_2') \cap \ldots \cup (x_m \cup x_m').$$

Upravme nyní tento výraz m-násobným použitím distributivního zákona. Dostaneme tak spojení m-členných průseků, kde do každého průniku je z každé závorky vzat jeden člen, t. j. buď x_i nebo x_i', $i = 1, 2, \ldots, m$, při čemž každá z proměnných se vyskytuje v každém z takto utvořených m-členných průseků jednou a jen jednou. Všech takových průseků, jež máme navzájem spojit, bude patrně tolik, jaký je počet m-členných kombinací s opakováním ze dvou prvků, t. j. 2^m. Jsou tedy uvažované průseky tyto:

$$(x_1 \cap x_2 \cap \ldots \cap x_m),\ (x_1' \cap x_2 \cap \ldots \cap x_m),$$
$$(x_1 \cap x_2' \cap \ldots \cap x_m), \ldots, (x_1' \cap x_2' \cap \ldots \cap x_m),$$
$$\ldots, (x_1' \cap x_2' \cap \ldots \cap x_m').$$

Spojení všech je funkce, nabývající neustále konstantní hodnoty j. Je snadno vidět, že každé dva různé z uvažovaných průseků mají za průsek nulu n (t. j. vlastně funkci, která se konstantně rovná n), neboť se zřejmě vždy vyskytne aspoň jedna proměnná x_i v jednom průseku bez doplňku a v druhém s doplňkem.

Vyberme nyní libovolnou skupinu z právě uvažovaných průseků a spojme průniky této skupiny. Dostáváme tak

celkem 2^{2^m} booleovských početních předpisů v úplné spojové normální formě; při tom nechť prázdná skupina našich průniků znamená formálně booleovskou funkci (konstantu), která nabývá stále hodnoty n. Tvrdím, že každý z těchto 2^{2^m} početních předpisů dává jinou booleovskou funkci. Dejme tomu, že naopak dvě různé úplné normální spojové formy dávají touž funkci

$$F(x_1, \ldots, x_m) = G(x_1, \ldots, x_m) \qquad (*)$$

pro všechny hodnoty proměnných, ale že v souhrnu průseků (činitelů spojení) úplné normální spojové formy $F(x_1, \ldots, x_m)$ postrádáme jeden z uvažovaných průseků, nazveme ho $p(\ldots)$, který však vystupuje ve vyjádření úplné normální spojové formy $G(x_1, \ldots, x_m)$ (jako člen spojení). (Na pořadí členů spojení nezáleží; aby však bylo určité, mohli bychom je dle vzoru úpravy racionální číselné funkce v úplné spojové normální formě také normovat lexikografickým způsobem uspořádání jednotlivých proměnných. Podrobnosti takové formální úpravy si čtenář laskavě provede jako snadné cvičení sám).

Protněme nyní obě strany prve napsané rovnosti (*) průsekem $p(\ldots)$. Za pomoci distributivního zákona snadno vidíme, že: Jednak vpravo zůstane průsek $p(\ldots)$ sám (průseky členu $p(\ldots)$ se všemi ostatními členy spojení $F(x_1, \ldots, x_m)$ jsou nuly n a ve spojení je ovšem vynecháme). A jednak nalevo dostáváme nulu n, jakožto spojení každého z našich základních průseků (vyskytujících se jako činitelé spojení v $F(x_1, \ldots, x_m)$ s průsekem $p(\ldots)$, který je od každého z nich různý). Avšak funkce $p(\ldots)$ sama nemůže dávat stále nulu n, neboť volíme-li $x_i = j$, jestliže se proměnná x_i vyskytuje ve funkci $p(\ldots)$ sama — a $x_k = n$ (čili $x'_k = j$), jestliže v $p(\ldots)$ vystupuje doplněk proměnné x_k, pak zaručeně nabývá funkce $p(\ldots) = p(x_1, \ldots, x_m)$ hodnoty $j \cap j \cap \ldots \cap j = j \neq n$. Ve skutečnosti snadno nahlížíme, že je to také jediná volba hodnot nezávisle proměnných $x_1, \ldots, x_m$, pro niž nabývá funkce $p(\ldots)$ hodnotu různou od nuly n. Tak na př. pro

$m = 3$ funkce $p(\ldots) = x_1' \cap x_2 \cap x_3'$ nabývá patrně hodnoty j jen pro $x_1 = n$, $x_2 = j$, $x_3 = n$.)

Máme tedy celkem 2^{2^m} různých booleovských funkcí (o m nezávisle proměnných na dvouprvkové algebře $B = (n, j)$) vyjádřeno jim odpovídajícími 2^{2^m} různými úplnými spojovými normálními formami. Avšak již víme, že všech Booleovských funkcí o m nezávisle proměnných vůbec definovatelných na dvouprvkové algebře je nejvýše 2^{2^m}.

Tedy jsme úplnou spojovou normální formou vyjádřili každou z uvažovaných booleovských funkcí, t. j. prvků Booleovy algebry A_m — a to jednoznačně. Algebra má tedy také skutečně A_m právě 2^{2^m} prvků. Abychom dokončili důkaz naší věty, stačí již dodat toto:

Je již zřejmo, že vztah svazového částečného uspořádání

$$f(x_1, \ldots, x_m) \subset g(x_1, \ldots, x_m)$$

pro dvě z našich booleovských funkcí bude splněn tehdy a jen tehdy, když skupina základních průseků — činitelů spojení (v úplné spojové normální formě pro funkci $f(\ldots)$) je vlastní (t. j. od celku různou) částí skupiny takových průseků — činitelů úplné spojové normální formy funkce $g(\ldots)$. Již z toho je vidět, že samotné průseky $p(\ldots)$, t. j. funkce dané průsekem všech proměnných, resp. jejich doplňků (při čemž se každá z m proměnných x_i vyskytuje právě jednou), jsou atomy naší algebry A_m. Dle již řečeného jsou atomy $p(\ldots)$ v A_m jakési základní booleovské funkce (o m nezávisle proměnnnných na algebře (n, j)), které nabývají hodnoty „jednotkové" j právě pro jednu jedinou m-člennou variaci s opakováním ze dvou prvků n, j, t. j. pro jeden jediný sled hodnot jednotlivých proměnných x_i $(i = 1, 2, \ldots, m)$ (všude jinde nabývají hodnoty „nulové" n).

Tím jsme dokázali naši větu a zároveň nabyli jakéhosi přehledu o prvcích naší algebry A_m booleovských funkcí. Rovněž jsme již s to nahlédnout, v čem tkví použitelnost to-

hoto druhu konečných algeber booleovských funkcí pro konečně kombinatorické úlohy vůbec. Všech vůbec možných způsobů, jakými lze jednoznačně konečným m-členným posloupnostem tvořeným vždy ze dvou prvků („nuly" n a „jednotky" j) přiřadit opět vždy buď jeden anebo druhý ze dvou prvků, „nulu" n anebo „jednotku" j je totiž — jak víme — právě 2^{2^m}. Vidíme tedy, že každé takové přiřazení, t. j. tabulka, přiřazující jednotlivým m-ticím sestaveným z členů n a j, opět vždy členy n anebo j, ať bylo docíleno jakýmkoli způsobem, dá se vždy vystihnout početní booleovskou formulí, dá se považovat za booleovskou („racionální") funkci. Dokonce lze vyjádřit takové přiřazení v úplné spojové normální formě booleovského početního předpisu. [Poznamenejme hned, že obdobná věta neplatí pro algebru všech booleovských funkcí na libovolné konečné Booleově algebře.] Co více, z tabulky pro booleovskou funkci vyčteme ihned její úplnou spojovou normální formu tímto způsobem:

Všimněme si jen řádků tabulky, jež končí jednotkovou hodnotou funkce. Jeden takový řádek nám dá ihned jeden z činitelů spojové normální formy. Nezávisle proměnnou, která v takovém řádku nabyla hodnoty jednotkové, vezmeme jako činitel průniku a k nezávisle proměnné, která nabyla nulové hodnoty v tomto řádku, vezmeme doplněk. Tak na př. z tab. 3, kde $n = 0$, $j = 1$ takto vyčteme ihned pro tam tabelovanou funkci o třech nezávisle proměnných $f(x_1, x_2, x_3) = (x_1 \cup x_2) \cap x_3'$ její úplnou spojovou normální formu jakožto

$$f(x_1, x_2, x_3) = (x_1 \cap x_2 \cap x_3') \cup (x_1 \cap x_2' \cap x_3') \cup \\ \cup (x_1' \cap x_2 \cap x_3').$$

(Doporučuji čtenáři, aby se o tom přesvědčil početní úpravou původně daného tvaru funkce.) Jako cvičení si čtenář dokáže obecnou správnost takovéhoto způsobu získávání úplné spojové normální formy pro booleovskou funkci na algebře (0,1). — V následujícím odstavci uvidíme, jak se tohoto užívá v elektrotechnice.

Poslední věta nám dokazuje existenci a jednoznačnost spojového úplného normálního vyjádření Booleovy funkce o konečném počtu nezávisle proměnných na dvouprvkové algebře (n, j). Nedává nám však prakticky početní postup, jak takovou Booleovu funkci, danou obecně libovolným početním Booleovým předpisem, na normální spojový tvar uvést. Praktický postup je dvojí: Buďto nepřímo, pomocí tabelace, právě uvedeným způsobem, anebo přímo takto: Nejprve užíva-

TABULKA FUNKCE

$f(x_1, x_2, x_3) = (x_1 \cup x_2) \cap x_3'$

x_1	x_2	x_3	$(x_1 \cup x_2) \cap x_3'$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

Tab. 3.

jíce (několikráte) obou pravidel De Morganových posouvejme postupně operaci doplňku stále dovnitř a upravme daný výraz naší funkce tak, až operace doplňku se již vesměs vztahují přímo na jednotlivé nezávisle proměnné x_i. Potom počněme odstraňovat pomocí distributivního a asociativního zákona komplikovanou kombinaci spojování a protínání takto: postupujíce od nejvnitřnějších výrazů (v jednoduchých závorkách), proveďme všechna případná naznačená protínání, která se pomocí distributivního zákona dají provést, t. j. převést na spojení průniků jednotlivých proměnných nebo jejich doplňků. Vkládajíce mezi tyto úpravy vynechávání přebytečných zá-

vorek (na podkladě zákonů asociativity) docílíme nakonec, že nám zůstane spojení několika průseků, kde členové průseku jsou buďto samy nezávisle proměnné x_i nebo jejich doplňky. Nyní ještě protneme tento výsledek postupně všemi takovými spojeními $x_k \cup x_k'$, že x_k chybí v některém z právě obdržených průniků. Tím se daná funkce nemění (protínáme ji funkcí, která je neustále rovna jednotce j) a dostaneme do vyjádření naší funkce spojením co nejjednodušších průseků všechny ty z proměnných, které tam dříve chyběly. Tím naše vyjádření dané booleovské funkce nabude tvaru úplné normální spojové normy. Na př. nechť

$$f(x_1, x_2, x_3) = (x_1 \cap x_2)' \cup x_3.$$

Úprava na normální spojovou formu probíhá takto:

$= x_1' \cup x_2' \cup x_3 = \| \cap (x_1 \cup x_1')$
$= (x_1 \cap x_2' \cup (x_1 \cap x_3) \cup x_1' \cup (x_1' \cap x_2') \cup (x_1' \cap x_3) = \| \cap (x_2 \cup x_2')$
$= (x_1 \cap x_2 \cap x_3) \cup (x_1 \cap x_2') \cup (x_1' \cap x_2 \cap x_3) \cup (x_1 \cap x_2') \cup (x_1 \cap$
$\cap x_2' \cap x_3) \cup (x_1' \cap x_2') \cup (x_1' \cap x_2 \cap x_3) = \| \cap (x_3 \cup x_3'),$
$= (x_1 \cap x_2 \cap x_3) \cup (x_1' \cap x_2 \cap x_3) \cup (x_1 \cap x_2' \cap x_3) \cup (x_1' \cap x_2 \cap x_3) \cup$
$\cup (x_1' \cap x_2 \cap x_3') \cup (x_1 \cap x_2' \cap x_3) \cup (x_1' \cap x_2' \cap x_3).$

Čtenář si sám zkontroluje početní postup a nalezne normální spojovou formu jiných booleovských funkcí (viz cvičení).

Větou o jednoznačnosti normální úplné spojové (po případě průnikové) formě pro každou booleovskou funkci na dvouprvkové booleově algebře jsme podali druhou hlavní poučku z theorie konečné Booleovy algebry. V obou hlavních větách o konečných Booleových algebrách jsme natolik nahlédli do jednoduché (ve srovnání na př. s konečnými grupami) povahy konečných Booleových algeber, že se dále již budeme moci stručně zabývat podstatou aspoň některých aplikací — a to: na elektrotechniku a na logiku.

Poznamenejme, že zvláště v aplikacích bývá vhodné brát pro určitost za oba prvky naší dvojprvkové Booleovy algebry číselnou nulu 0 — a považovat ji rovněž za nulu ve smyslu booleovy algebry — a číselnou jednotku 1 — a rovněž ovšem ji považovat též za jednotku ve smyslu dvouprvkové booleovy algebry $B = (0, 1)$. Vedle jiných výhod má to i tu přednost, že booleovské úkony v algebře (0, 1) možno považovat za takto zavedené číselné úkony:

Označme na okamžik jako $\langle x \rangle$ pro celé číslo x nejmenší nezáporný zbytek čísla x děleného 2. (Je tedy $\langle x \rangle = 1$, jakmile je x liché a $\langle x \rangle =$

$= 0$ jakmile je x sudé.) Pak můžeme psát v algebře (0, 1) (a i b může být jen 0 nebo 1)

$$a \cup b = \langle a + b + ab \rangle,$$
$$a \cap b = ab,$$
$$a' = \langle a + 1 \rangle.$$

Cvičení k 2,6.

1. Vyjádřete v úplné normální spojové formě nejjednodušší booleovské funkce o m nezávisle proměnných (na algebře (n, j))

$f_j(x_1, \ldots, x_m) = x_j$
$g_j(x_1, \ldots, x_m) = x'_j$
$h_{i,j}(x_1, \ldots, x_m) = x_i \cup x_j$
$k_{i,j}(x_1, \ldots, x_m) = x_i \cap x_j$ (volte na př. $m = 5$).

2. Totéž, co v 1— pro úplnou průnikovou normální formu (duálně)

3. Tabelujte dle vzorců tab. 2 a 3 tyto booleovské funkce o třech nezávisle proměnných

a) $f(x_1, x_2, x_3) = (x_1 \cap x'_2) \cup (x'_3 \cap x_1)$.
b) $g(x_1, x_2, x_3, x_4) = (x_1 \cap x_2) \cup x_3 \cup x'_4$.

Najděte (dle způsobu, udaného v textu) jejich úplné spojové normální formy a přejděte k úplným průsekovým normálním formám dualisací.

4.*Odůvodněte podrobně (pomocí věty o úplné spojové normální formě) v textu udaný způsob, jak z tabelace booleovské funkce vyčíst její úplnou spojovou normální formu.

2,7. PRINCIP APLIKACE THEORIE BOOLEOVÝCH ALGEBER V ELEKTROTECHNICE.

Hlavní aplikace theorie Booleových algeber v elektrotechnice se týkají t. zv. reléově-kontaktních systémů. Příkladem takového jednoduchého systému je t. zv. Wagnerovo kladívko, jež pohání elektrický zvonek. Příkladem složitého takového systému je telefonní centrála nebo elektromagnetický matematický stroj.

Princip činnosti a účel reléově-kontaktního systému možno popsat takto: Na kteroukoli určitou kombinaci zapojení a vypojení pevného počtu m t. zv. *vstupních* (dvoupolo-

hových) klíčů (ať již jsou ovládány mechanicky nebo ručně), což představuje zvenčí přicházející popud, reaguje relátkově-kontaktní systém tím, že v jistých t. zv. *výstupních* větvích, čili stručně *ve výstupech*, jednak zapojuje a jednak vypíná proud.

Při tom je třeba rozeznávat t. zv. *jednotaktní* a *mnohotaktní* systémy. Jednotaktní systém na určitou kombinaci zapojení a vypojení vstupních klíčů odpovídá jedinou (vždy stejnou) kombinací propouštění a nepropouštění proudu současně v jednotlivých výstupech. Příkladem je třeba elektromagnetický zámek „na heslo", který na určitou jednu, po případě několik málo kombinací stisků většího počtu vstupních tlačítek („hesel") elektromagneticky otevírá zámek, na každou jinou vyvolává poplach.

Naproti tomu mnohotaktní reléově-kontaktní zařízení je takové, kde určitá kombinace zapojení vstupních klíčů může vyvolat celý časový sled střídajících se kombinací propouštění a přerušení proudu ve výstupech. Nejjednodušším příkladem je tu již uvedené Wagnerovo kladívko, kde sled taktů práce zařízení spočívá v theoreticky neomezeném zapojování a přerušování proudu v jediném výstupu, na popud stisku jediného vstupního klíče.

Práce reléově-kontaktního systému je prováděna zpravidla soustavou elektromagnetických kontaktních relé (t. zn. elektromagnetů s kotvou, která je odtahována vzpružinou a která ovládá jeden nebo více kontaktů, t. j. přitažením kotvy buďto zapojuje, nebo naopak rozpojuje elektromagneticky řízený kontakt). Tak právě zapojená větev systému, která je pod proudem, zapojuje (vypojuje) jinou větev systému, až posléze postupně dojde k zapojení nebo vypojení proudu ve výstupech celého systému.

Úlohu elektromagnetických kontaktních relé jakožto elektricky řízených zapojovačů a vypojovačů proudu mohou však také v daném případě vykonávat mnohem rychleji vhodné elektronky, což se děje zejména v matematických elektrických strojích. Aplikace Booleovy algebry se právě tak týká i systémů, pracujících s elektronkami

na místě elektromagnetů. Nicméně se přidržíme elektromagnetických reléově-kontaktních systémů.) Při vícetaktních zařízeních určité nastavení vstupních klíčů vyvolá jistou kombinaci spojení a rozpojení proudu ve výstupech — v prvním taktu práce. (U jednotaktního systému by tím byla práce systému ukončena.) V zápětí nato některé nebo všechny výstupní větve spustí jistá elektromagnetická kontaktní relé uvnitř systému, která zapojí či rozpojí některé jeho větve. Tím se celé zařízení změní a připraví k druhému taktu práce. V druhém taktu se pak objeví ovšem ve výstupech obecně jiná kombinace rozpojení a zapojení proudu; ta opět (obecně) elektromagneticky změní zapojení uvnitř zařízení — a to se může opakovat konečně mnoho, nebo i (theoreticky) nekonečně mnohokrát.

Dále se omezíme jen na nejjednodušší případ, t. j. na *jednotaktní reléově-kontaktní zařízení s jedním výstupem*, říkejme krátce *jj-zařízení* (*jj*-systémy). Ty tvoří základní „články" reléově-kontaktních elektromagnetických zařízení a základní prostředky z theorie Booleovy algebry k aplikaci na tento nejjednodušší případ máme dány předchozím výkladem.

Činnost, resp. úlohu, *jj*-zařízení můžeme matematicky popsat takto: Fakt, že byl zapojen (vypojen) i-tý z m vstupních klíčů vy jádříme tím, že i-tá proměnná x_i nabyla hodnoty 1 (0). Výsledku činnosti *jj*-zařízení, t. j. zapojení anebo vypojení proudu ve výstupu, dáme opět výraz hodnotou buďto 1 anebo 0, které takto nabývá jistá závisle proměnná, řekněme X.

Tak se nám jeví každé *jj*-zařízení jako způsob, jakým je libovolné m-tici, složené z čísel 0, 1, přiřazeno jednoznačně opět číslo 0 nebo 1. Činnost *jj*-zařízení (co do účinku) můžeme pak prostě vystihnout tabulkou o 2^m řádcích a $m + 1$ sloupcích, kde v každém řádku je nejprve zanesena m-tice sestavená z 0 a 1 (kombinace zapojení a vypojení vstupních klíčů) a na konci (v posledním sloupci) je opět číslo 0 nebo 1 (výsledné zapojení nebo rozpojení výstupu).

V předchozím paragrafu jsme se však dověděli, že každý takový způsob, přiřazující libovolné m-tici z čísel 0, 1 přesně jedno z čísel 0, 1, lze vyjádřit booleovským početním předpisem, že takové přiřazení je booleovská funkce na algebře

0, 1. Lze tedy každé uskutečněné *jj*-zařízení považovat za elektrotechnickou realisaci booleovské funkce o m nezávisle proměnných (a jedné závisle proměnné hodnotě funkce). Tabulka takové funkce je právě tabulkou práce odpovídajícího *jj*-zařízení.

Z předchozího paragrafu je nám známo, že jedna a táž booleovská funkce (závislost udaná toutéž tabulkou) může být dána různými ekvivalentními početními předpisy (výrazy).

Nazývejme proto důsledně *jj-zařízením* elektromagneticky realisovanou booleovskou funkci (závislost) proměnné X na nezávisle proměnných $x_1, x_2, \ldots, x_m$. Naproti tomu termín *jj-systém* si ponechme pro způsob, jak takové zařízení uskutečnit, t. j. pro příslušné elektrické zapojení. To tedy znamená, že slovo zařízení nám značí pouze způsob, jak systém reaguje, nikoliv jeho elektrotechnickou výstavbu, kterou právě označujeme názvem *jj*-systém. Máme tedy vzájemně jednoznačné odpovídání si mezi *booleovskými funkcemi* o m nezávisle proměnných na algebře 0, 1 a mezi *jj-zařízeními* o m vstupních klíčích a jediné výstupní větvi, které je dáno společnou tabulkou pro funkci a pro výsledek činnosti (úlohu) *jj*-zařízení. Naproti tomu mnohost početních vyjádření téže booleovské funkce (na algebře 0, 1) různými početními předpisy odpovídá mnohosti elektrotechnických systémů (zapojení) pro jedno a totéž *jj*-zařízení.

Při tom jsme ovšem mlčky učinili zásadní předpoklad, že každé tabulkou žádané *jj*-zařízení lze opravdu elektrotechnicky realisovat (po případě jen theoreticky, v praxi ovšem nemůžeme na př. realisovat zařízení o 10^{100} vstupních klíčích, t. j. booleovskou funkci 10^{100} nezávisle proměnných). — Odůvodnění tohoto předpokladu si podáme za chvíli.

Zatím však můžeme již blíže a přesněji říci, v čem spočívá princip aplikace theorie Booleových algeber na theorii *jj*-zařízení.

Jak známo, booleovské funkce na algebře 0, 1 samy tvoří

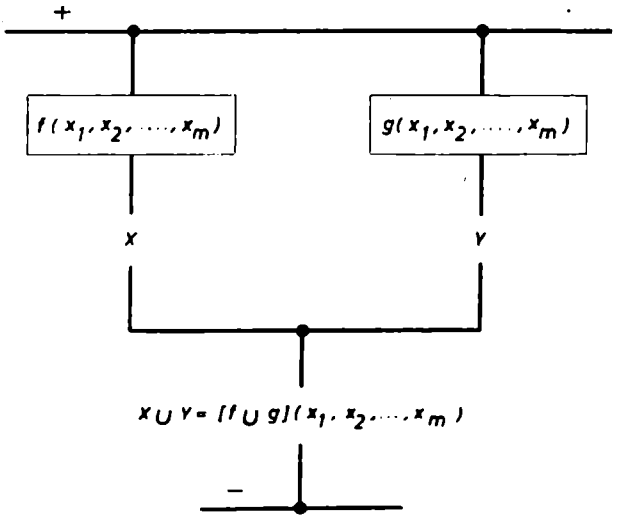
jistou Booleovu algebru (jde-li o funkce o m nezávisle proměnných, má tato algebra, jak víme 2^{2^m}, prvků). Co rozumíme v této algebře spojením $[f \cup g](x_1, \ldots, x_m)$ a co rozumíme průsekem $[f \cap g](x_1, \ldots, x_m)$ dvou booleovských funkcí $f(x_1, \ldots, x_m)$ a $g(x_1, \ldots, x_m)$ o m nezávisle proměnných $x_1, \ldots, x_m$? Jsou to funkce, které pro danou m-tici hodnot nezávisle proměnných $x_1, \ldots, x_m$ nabývají hodnoty, dané spojením, resp. průnikem obou hodnot daných funkcí, t. j. jsou to tedy funkce z nichž první nabývá hodnoty 1 tehdy a jen tehdy, když alespoň jedna ze (spojovaných) funkcí f a g nabývá hodnoty 1; druhá je funkcí, která nabývá hodnoty 1 tehdy a jen tehdy, když obě (z protínaných) funkcí f a g nabývají hodnoty 1; konečně doplněk $f'(x_1, \ldots, x_m)$ (booleovské funkce m nezávisle proměnných) je funkce, která nabývá hodnoty 0 resp. 1 tam, kde funkce $f(x_1, \ldots, x_m)$ nabývá hodnoty 1, resp. 0.

Považujeme-li tedy samotná uskutečnění *jj*-zařízení za elektrotechnicky realisované booleovské funkce, můžeme říci, že svazovým spojením dvou již realisovaných *jj*-zařízení je takové *jj*-zařízení, které ve svém výstupu vede proud přesně při takovém nastavení vstupních klíčů (společných pro obě daná *jj*-zařízení), při němž projde proud výstupem aspoň jednoho z daných zařízení. Podobně za svazový průsek dvou již realisovaných *jj*-zařízení nutno považovat takové *jj*-zařízení, jež svým výstupem propouští proud tehdy a jen tehdy, jsou-li pod proudem oba výstupy daných *jj*-zařízení. Konečně za svazový doplněk již realisovaného *jj*-zařízení je třeba považovat takové *jj*-zařízení, jež propouští proud svým výstupem tehdy a jen tehdy, když v daném zařízení je výstup rozpojen, a rozpojí ve svém výstupu proud přesně tehdy, když výstup daného zařízení je pod proudem.

Jde tedy o to, jak elektrotechnicky realisovat svazové spojení, svazový průsek a svazový doplněk již realisovaných *jj*-zařízení.

Zvláště prostá je realisace *svazového spojení a svazového průseku*. Dejme tomu, že máme *jj*-systém, realisující funkci

$f(x_1, \ldots, x_m)$ a jj-systém, realisující funkci $g(x_1, \ldots, x_m)$. Nechme systém pro $f(x_1, \ldots, x_m)$ elektromagneticky řídit kontakt, vložený do vodiče X (tak, že X je spojen tehdy a jen tehdy, když vede výstup systému pro $f(x_1, \ldots, x_m)$. (Podobně pro vodič Y a funkci $g(x_1, \ldots, x_m)$. Na to oba vodiče připojme *paralelně* (vedle sebe) k témuž zdroji proudu (obr. 22) — to



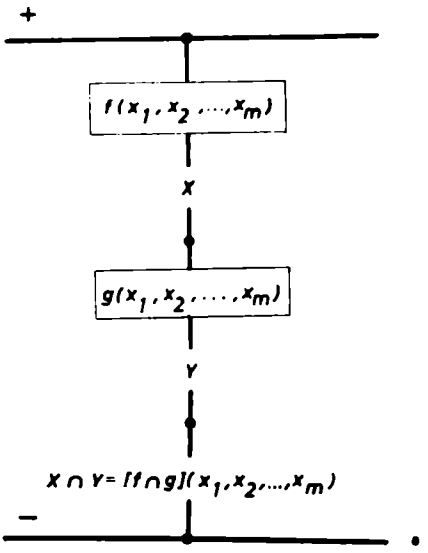
Obr. 22.

pro případ realisace *svazového spojení* — a *do serie* (za sebou) — to pro případ realisace *svazového průseku* (viz obr. 23). Je jasno, že výstupní větev, jíž je takto sestrojený jj-systém ukončen, představuje podle toho zda je pod proudem nebo bez proudu obě možné hodnoty Z závisle proměnné $Z = [f \cup g](x_1, \ldots, x_m)$ — to v případě spojení a $Z = [f \cap g](x_1, \ldots, x_m)$ — to v případě průniku.

Konečně *svazový doplněk* booleovské funkce $f(x_1, \ldots, x_m)$,

pro níž již máme realisující jj-systém, realisujeme elektrotechnicky takto:

Do výstupní větve X systému realisujícího $f(x_1, \ldots, x_m) = X$ vložíme cívku elektromagnetického relé, které v jistém vodiči (větvi) Y přitažením kotvy vypíná pomocný



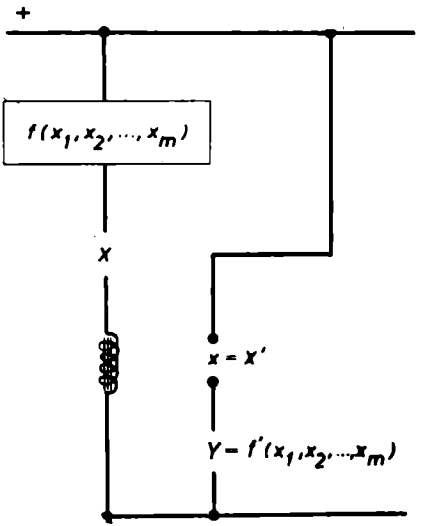
Obr. 23.

kontakt x a tím *rozpojuje* výstupní větev $Y = X'$ právě a jen když větví X prochází proud, kdežto neprochází-li proud větví X, pak puštěná kotva na vzpružině zapojuje proud v Y (viz obr. 24).

(Není podstatné, že ve všech třech případech napájíme původní a nové výstupy ze stejného zdroje proudu. Dále je třeba si uvědomit, že uvedený způsob elektrotechnické realisace základních úkonů v Booleově algebře funkcí (o m

nezávisle proměnných na algebře (0, 1)) není jediný možný. Tak na př. na obr. 25 je naznačen prostý způsob, jak realisovat funkci $f(x_1, x_2) = (x_1 \cap x_2') \cup (x_1' \cap x_2)$ bez elektromagnetických relé, pouhou mechanickou vazbou kontaktů.)

Vraťme se nyní krátce k předpokladu, jehož zaručení dlužíme, že totiž (a jak) každá booleovská funkce, t. j. každé

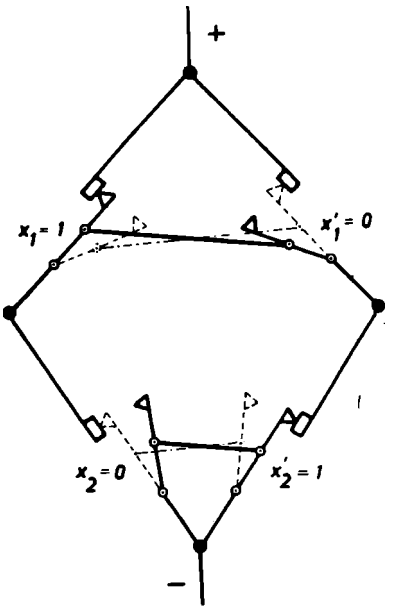


Obr. 24.

předepsané *jj*-zařízení, se opravdu dá realisovat. (Tím teprve bude ukázána alespoň jedna základní theoretická aplikace našich poznatků z theorie Booleových algeber.)

V minulém paragrafu jsme se naučili, jak z tabulky pro booleovskou funkci vyčíst pomocí úplné normální spojové formy početní vyjádření takové funkce (které není vždy nejjednodušší). Jak víme, v této formě se každá (sebesložitější)

booleovská funkce (s výjimkou té, jež nabývá stále hodnoty nula) jeví jako spojení několika funkcí, z nichž každá je nenulovým průnikem všech m nezávisle proměnných, resp. jejich doplňků (tyto průniky představují atomy Booleovy algebry funkcí m nezávisle proměnných na algebře (0, 1)).



Obr. 25.

Protože už víme, jak elektrotechnicky realisovat spojování, protínání a doplněk těchto booleovských funkcí, je beze všeho patrno, že způsob jak z tabulky booleovské funkce vyčíst její úplnou spojovou normální formu elektrotechnicky čten znamená vlastně přímo návrh na *jj*-systém, realisující *jj*-zařízení, jehož práce je předepsána zmíněnou tabulkou.

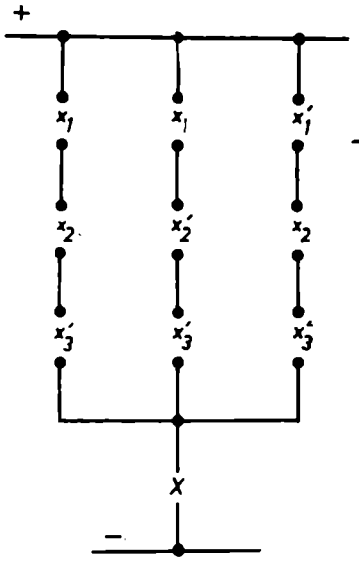
(Každé nezávisle proměnné x_i v normální spojové formě přiřadíme jeden vstupní dvojpolohový klíč. Každému *výskytu* proměnné x_i v každé normální spojové formě přiřadíme jeden kontakt. Klíč pro x_i (i-tý vstupní klíč) současně ovládá všechny t. zv. vstupní kontakty, odpovídající místům výskytu proměnné x_i; každý klíč ovládá tedy tolik vstupních kontaktů, kolik je činitelů spojení ve spojové normální formě.

Klíč pro x_i má dvě polohy: pro $x_i = 1$ a pro $x_i = 0$. V poloze pro $x_i = 1$ zapojuje všechny kontakty pro všechny výskyty x_i a rozpojuje všechny kontakty pro všechny výskyty x_i'. Každému činiteli spojové normální formy pak odpovídá m v serii zapojených kontaktů, příslušných k x_i resp. x_j', které vystupují v jednom činiteli ($i, j = 1, 2, \ldots, m$). Celé normální spojové formě pak odpovídá paralelní spojení všech těchto seriových spojení. Konečně napojením ze společného zdroje jsme získali t. zv. seriově-paralelní *jj*-systém pro tabulkou předepsané *jj*-zařízení, který přesně odpovídá svou výstavbou úplné spojové normální formě odpovídající funkce (jestliže jsme ještě vložili za vypsané paralelně seriové zapojení kontaktů výstupní větev, odpovídající hodnotě závisle proměnné v dané funkci). (Viz obr. 26a, ukazující schema systému pro realisaci funkce z tabulky 3. v její úplné spojové normální formě.)

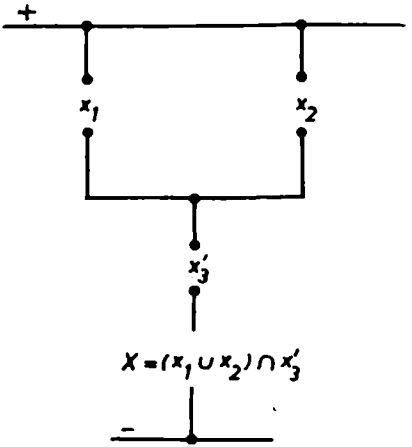
Vidíme tedy, že zásadně dovedeme pro žádané *jj*-zařízení vždy udat *jj*-systém, který jej realisuje a přesně odpovídá úplné spojové normální formě. Takový systém ovšem zdaleka nebývá vždy jednoduchý a praktický. Tak na př. na obr. 26b je schema pro jednodušší výraz funkce z obr. 26a. Vyvstává tedy prakticky nejdůležitější úloha tento systém přetvořit a zjednodušit *v systém s ním ekvivalentní*, t. j. *realisující totéž jj-zařízení*, tutéž booleovskou funkci, ale způsobem co nejjednodušším, po případě technicky vymezeným.

Toho se dosáhne takto: Technicky důležitým praktickým způsobům zapojení čili *jj*-systémům necháme vzájemně jed-

noznačně odpovídat vhodné početní výrazy (jiné, než spojové normální formy). Pak vlastní práce při praktické aplikaci Booleově algebry spočívá v hledání vhodné formy pro danou booleovskou funkci, v přetváření již daného výrazu pro funkci ve výraz hledaného tvaru. Zatím co dosud jsme se seznámili jen se *seriově paralelními systémy*, jsou v praxi dů-



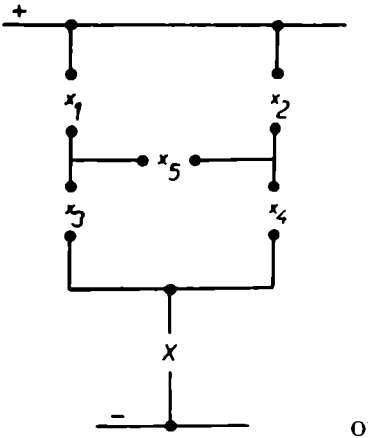
Obr. 26a.



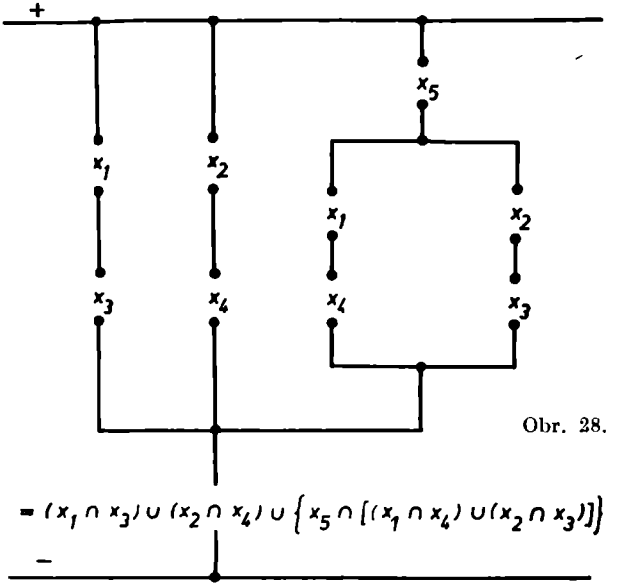
Obr. 26b.

žitá i jiná, t. zv. *můstková* zapojení, která přímo realisují některé složitější booleovské funkce, resp. jejich výrazy. Příklad máme na obr. 27, kdežto na obr. 28 je zřejmě neprakticky složité k můstku ekvivalentní seriově paralelní zapojení.

Tolik tedy k tomu, aby si čtenář učinil představu, jak se alespoň v nejjednodušších případech užívá Booleovy algebry


+
x_1
x_2
x_5
x_3
x_4
X
−

Obr. 27.


+
x_5
x_1
x_2
x_1
x_2
x_3
x_4
x_4
x_3
$= (x_1 \cap x_3) \cup (x_2 \cap x_4) \cup \{x_5 \cap [(x_1 \cap x_4) \cup (x_2 \cap x_3)]\}$
−

Obr. 28.

k návrhu, rozboru a zjednodušování reléově kontaktních systémů. Třebaže Booleova algebra — jako vůbec každá aplikace matematiky v technice — nedává ani zde zázračný a mechanicky aplikovatelný recept pro všechny případy, přece značně usnadňuje sestrojování a zkoušení reléově kontaktních systémů, které se dříve hledalo pracnou více méně pokusnou cestou. V dalších otázkách musím ovšem odkázat čtenáře na citovanou *Gavrilovovu* knihu.

Cvičení k 2,7.

1. Udejte schema systému pro elektrickou realisaci booleovské funkce, dané tabulkou:

a)

x_1	x_2	$f(x_1, x_2)$
1	1	1
1	0	1
0	1	0
0	0	1

b)

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

2. Udejte seriově paralelní schema pro některé z t zv. selektivních *jj*-zařízení; to jsou taková, že propouštějí proud právě a jen když je zapojen pevný počet r libovolných klíčů (z celkového počtu m klíčů). Tak na př. tabulka selektivního zařízení pro $r = 2$, $m = 3$ je taková:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Zjednodušte schema co nejvce úpravou výrazu pro danou funkci.

3.*Využijme toho, že konečné posloupnosti z čísel 0, 1 odpovídají vzájemně jednoznačně celým číslům, psaným ve dvojkové čili dyadické soustavě. Pak sečítání dvou čísel (ve dvojkové soustavě) je vlastně vystiženo tolika booleovskými funkcemi na algebře 0, 1, kolik dyadických míst má součet (t. j. nejvýše o jedno více než jich má větší z obou čísel). Dyadické místo součtu, t. j. 0 či 1, je totiž patrně hodnotou jisté booleovské funkce, jejímiž nezávisle proměnnými se jeví být jednotlivá čísla dvojkového rozvoje obou sčítanců v daném místě a napravo od něho. k-té místo součtu dvou čísel ve dvojkové soustavě (0 nebo 1) (od konce vzato) je tedy hodnotou booleovské funkce nejvýše $2k$ nezávisle proměnných na algebře (0,1). Celý součet dvou obecných sčítanců až do jisté velikosti tedy dán konečnou posloupností určitých takových funkcí, jež mají společné některé nezávisle proměnné; dále jež hodnotami svých závisle proměnných udávají jednotlivá dydická místa součtu; a konečně jichž je tolik, kolik může mít součet míst.

Tak je dána zásadní možnost elektricky realisovat sečítání ve dvojkové soustavě tím, že elektricky současně realisujeme všechny booleovské funkce pro všechna místa součtu, pro tak veliká čísla, jak to potřebujeme.

Úkolem čtenáře je pokusit se na podkladě těchto poznámek udat booleovské funkce a navrhnout schema pro elektrické sečítání dvou, řekněme nejvýše šestimístných čísel (ve dvojkové soustavě), čili čísel nejvýše rovných $2^6 = 64$. Nechť si čtenář uvědomí, že způsob takového elektrického počítání je tím *zásadně* odlišný od běžného postupného zjišťování míst součtu pomocí přenosu (ve dvojkové soustavě), že zařízení pro elektrické sčítání „umí" udat součet *najednou na všech* (dvojkových) *místech*. Takový sečítající systém si může čtenář pro malý počet míst a dva sčítance prakticky sestrojit pomocí pouhých několika kapesních baterií, vhodně upravených obyčejných vypinačů a tolika žárovek (jakožto indikátorů proudu ve výstupech) kolik nejvýše je dvojkových míst součtu. — Žárovka svítí: příslušné místo součtu je 1; žárovka nesvítí: příslušné místo součtu je 0.) Podobně si může čtenář sestrojit (složitější) elektrické schema pro *násobení* dvou nevelkých, dvojkově rozvedených celých čísel. (V praxi elektrických počitacích a matematických strojů se ovšem užívá z technických důvodů jiných, při velkých číslech praktičtějších elektrických realisací sečítání a násobení releově-kontaktními systémy.)

2,8. APLIKACE BOOLEOVY ALGEBRY NA VÝROKOVOU (THEORETICKOU) LOGIKU.

Theoretická výroková logika (kterou odlišujeme od praxe každodenního používání logiky) je základní a nejjednodušší částí theoretické logiky. Nazýváme-li matematickou logikou takovou theoretickou logiku, která užívá matematických method ke studiu logických vztahů, pak výroková matematická logika je jejím prototypem a v aplikaci na ni se vlastně historicky Booleova algebra objevila.

Oč jde ve výrokové logice, to můžeme stručně a poněkud zhruba charakterisovat takto:

Výroková logika zkoumá vztahy mezi větami libovolného jazyka (řeči), pokud se tyto vztahy zakládají na následujících třech předpokladech.

Předně, věty považujeme za blíže nedefinované a samostatně o něčem vypovídající skupiny výrazů řeči; při tom výroková logika rozeznává jednak: t. zv. *jednoduché věty* jako jsou na př. „Zítra bude hezky", „Všichni lidé jsou si rovni", „$2 + 3 = 6$", atp. — označujme je malými písmeny $a, b, c, \ldots$

Dále rozeznáváme od jednoduchých vět t. zv. *složené věty* (souvětí), jež jsou budovány postupně z jednoduchých vět pomocí (jedno či vícenásobným kombinováním) t. zv. *logických spojek*:

Spojka $\vee$ (*nebo*, lat. vel), spojka & (lat. et, souřadné *a*), spojka $\rightarrow$ (implikační, pro podmínečné souvětí „Když..., pak..." a konečně záporka $\sim$ (Ne, nikoli, lat. non, též se opisuje rčením „Není pravda, že...) (Věty vůbec (složené i jednoduché) označujme velkými písmeny $A, B, C, \ldots$). Tak na př. je-li $a =$ „Zítra bude hezky", $b =$ „Zítra půjdu na vycházku", $c =$ „Každý člověk zemře" pak $A = a \vee b$ značí: „Zítra bude hezky nebo půjdu na vycházku" $a \rightarrow b = B$ značí: „Když bude zítra hezky, pak půjdu na vycházku" $\sim c$ značí: „Ne každý člověk umře ($\doteq$ není pravda, že

každý člověk zemře)". Můžeme však též utvořit souvětí $a \rightarrow \sim c$ (t. j. „Když bude zítra hezky, pak ne každý člověk zemře". Je třeba zdůraznit, že pro výrokovou logiku jsou jednoduché výroky již dále nerozložitelnými elementy. Protože výroková logika nebere (a není také s to brát) ohled na reálnou náplň a smysl jednotlivých vět, a pak pro úplný přehled o všech theoreticky zásadně možných souvětích (právě udaného druhu), můžeme logickými spojkami ve výrokové logice bez omezení spojovat jakékoli dvě věty (složené či jednoduché). Tak na př. je-li $A = a \,\&\, b$, $B = c \vee b$, pak bereme ohled i na souvětí třebas $c = A \rightarrow B = (a \,\&\, b) \rightarrow (c \vee b)$ (t. j. „Když zítra bude hezky a zároveň půjdu na vycházku, pak: buď každý člověk zemře, nebo bude zítra hezky" (nebo obojí). (Rozumí se, že duševně normální lidé taková souvětí netvoří.)

Za druhé, výroková logika, aniž by mohla (jak již řečeno) se zabývat smyslem vět, je s to něco vypovídat pouze o jejich *pravdivosti* nebo *nepravdivosti*. Při tom se přijímá předpoklad, že každá věta je vždy buďto pravdivá, anebo nepravdivá. Můžeme říci, že každá věta může nabýt jedné a jen jedné „hodnoty pravdivosti": je-li věta A pravdivá, pak nabývá hodnoty 1, je-li věta A nepravdivá, nabývá hodnoty 0. (V tom je obsažena *zásada vyloučeného sporu* („principium contradictionis") a *zásada „tertium non datur"* (*vyloučeného třetího*) tradiční logiky.)

Při tom hodnota pravdivosti složeného výroku je *jednoznačně určena hodnotami pravdivostí* jeho složek. (To je t. zv. *zásada extensionality*.)

(Poznamenejme hned, že jsou intensivně studovány obecnější systémy výrokové logiky, v nichž není ani jedna z těchto zásad 1 a 2 přijímána; také v takových logikách (kde na př. neplatí zásada, že každá věta buďto je pravdivá, anebo není pravdivá) je theorie svazů důležitým matematickým nástrojem. Svazy, kterých je tam zapotřebí, jsou pak různě zobecněnými Booleovými algebrami.)

A konečně za třetí, elementární výroková logika stanoví logické hodnoty složených vět na základě předpokládaných logických hodnot částí podle těchto předpisů:

a) Věta $\sim A$ (nikoli A) je pravdivá tehdy a jen tehdy, když věta A je nepravdivá.

b) Věta $A \vee B$ (A nebo B) je nepravdivá, když a jen když jsou obě dvě věty A i B nepravdivé.

c) Věta $A \,\&\, B$ (A a B) je pravdivá tehdy a jen tehdy, když obě dvě věty A i B jsou pravdivé.

d) Věta $A \rightarrow B$ (když A, pak B) je nepravdivá tehdy a jen tehdy, když věta A (t. zv. implikans) je pravdivá a věta B (t. zv. implikát) je nepravdivá.

Shrneme-li na podkladě zásady o vyloučeném třetím a vyloučeném sporu právě udané předpisy pro stanovení hodnot pravdivosti souvětí pomocí daných hodnot pravdivosti jednotlivých jeho částí do přehledných, t. zv. Schröderových tabulek, pak vypadají takto:

A	$\sim A$
1	0
0	1

A	B	$A \vee B$	$A \,\&\, B$	$A \rightarrow B$
1	1	1	1	1
1	0	1	0	0
0	1	1	0	1
0	0	0	0	1

Vidíme tedy (srov. tab. na str. 162), že na základě právě vytčených tří základních předpokladů výrokové logiky lze na věty (složené i jednoduché) hledět jako na proměnné prvky z algebry (0, 1) hodnot pravdivosti, při čemž jednoduché věty jejichž pravdivost neznáme, se nám takto jeví jako nezávisle proměnné, složené věty jako závisle proměnné a tvoření složených vět (logických souvětí) jako tvoření složených Booleovských početních předpisů; příslušná Booleovská funkce, daná takto složenou větou, bude vhodně nazvána výpovědí, (která je vyjádřena touto danou (složenou) větou.)

Jak je zřejmo, jedna a táž výpověď (či tvrzení) může být vyjádřena různými, jak se říká, logicky ekviva-

lentními větami. [Na př. větu „Není pravda, že není pravda, že zítra bude hezky" — čili $\sim (\sim a)$, považujeme za logicky ekvivalentní s větou a — „Zítra bude hezky". Souvětí „Když bude zítra hezky, pak půjdu na vycházku" — $a \rightarrow b$ považujeme za větné vyjádření výpovědi, která by však mohla být právě tak dobře vyjádřena větou $\sim a \vee b$ — „Zítra ráno nebude hezky, nebo půjdu na vycházku".] Toto pak zcela odpovídá okolnosti, že jedna a táž booleovská funkce může být vyjádřena různými booleovskými početními předpisy. Při tom základní početní booleovské úkony jsou ve výrokové logice dány užitím uvedených logických spojek takto: Svazové *spojování* pomocí spojky $\vee$ (...nebo...) čili t. zv. *logické disjunkce*, svazové *protínání* pomocí spojky & (... a ...), t. zv. logické *konjunkce*, svazový *doplněk* pomocí *negace* $\sim$ (Nikoli...) *Podmínečné souvětí* $a \rightarrow b$ — jež je třeba pečlivě odlišovat od podmínečného vztahu, či vztahu důsledku mezi dvěma větami a a b — nám pak představuje *spojení doplňku prvního daného členu s druhým daným členem*. Můžeme se tedy na *symbolický zápis složeného souvětí* přímo dívat jako na *výraz pro booleovský početní předpis*, jestliže nám jen znak $\vee$ vyznačuje svazové spojování, znak & svazové protínání, znak $\sim$ svazový doplněk.

K čemu je taková „algebraisace" výrokové logiky? Všechna odvozená logická pravidla pro logickou ekvivalenci dvou složených vět po takové algebraisaci se jeví jako prostá aplikace axiomů Booleovy algebry a na základě nich je odvozujeme vhodnou početní úpravou početního Booleova předpisu, daného jednou větou, v booleovský početní předpis pro tutéž funkci (výpověď), který je daný druhou větou. Jinak řečeno, logické ekvivalence („rovnice" výrokové logiky) přecházejí, jak se ukazuje, v identické rovnosti (platné pro jakékoli dosazené prvky) v Booleově algebře (0, 1) — a ovšem i obráceně, každá taková identita značí logickou ekvivalenci. Tak na př. druhé z De Morganových pravidel Booleovy algebry vyjadřuje tento odvozený princip (poučku), vý-

rokové logiky: Říci, že není pravda, že současně A i B je logicky totéž, jako říci, že buď není pravda A, nebo není pravda B (nebo obojí).

Poznamenejme ještě, že ovšem poučky, které jsme si odvodili pro konečné Booleovy algebry, vesměs skýtají odpovídající poučky výrokové logiky. Tak se zejména ukazuje, že všechny (složené) výpovědi, jež lze učinit za pomoci m daných jednoduchých vět, tvoří Booleovu algebru o 2^{2^m} prvcích, t. j. výpovědech. Dále se ukazuje, že složená souvětí lze převádět na jednoznačně určené úplné spojové, zde je lépe říci *disjunkční* normální formy. To jsou s danou (složenou) větou logicky ekvivalentní souvětí, tvořená pomocí opakované spojky *nebo*; jeho částmi jsou opět souvětí tvořená vždy z různých daných m jednoduchých vět a jejich negací — pomocí souřadných spojek a. Co více, na takové úplné normální disjunkční formě pro dané souvětí máme možnost se přesvědčit, zda dané souvětí je, či není t. zv. tautologií, to jest souvětím „samozřejmě", bezpodmínečně pravdivým [které na jakékoli rozložení hodnot pravdivosti u nezávisle proměnných (jednoduchých vět) dává vždy konstantní hodnotu 1]. Jednoduché příklady tautologií: $a \vee \sim a$, $\sim(\sim a) \rightarrow a$, $a \rightarrow (a \vee b)$, a pod. Jak již nyní čtenář sám nahlíží, tautologie budou zřejmě všechny ty složené věty, jejichž úplná normální disjunkční forma je ta nejdelší pro Booleovskou funkci, identicky nabývající stále hodnoty 1.

Booleova algebra tedy skýtá matematický prostředek, jak o daném komplikovaném souvětí rozhodnout, zda je, či není tautologií, a to naprosto mechanisovatelným způsobem (vhodnou početní úpravou). (K tomu účelu dává ovšem Booleova algebra i jiné úspornější a praktičtější prostředky než je ten, který se opírá o úplnou spojovou normální formu; o těch zde však se již nelze šířit.) Lze říci, že prostě Booleova algebra řeší jednoduchým způsobem veškeré úkoly, jež se kladou elementární výrokové logika.

Tolik tedy ve vší stručnosti o aplikacích theorie (konečných) Booleových algeber na logice — a tolik o aplikacích theorie Booleovy algebry vůbec.

Na zakončenou si přehledně zopakujeme zvláště názorný, přímo školsky instruktivní příklad na různé, ale vzájemně isomorfní svazy, který nám poskytují konečné Booleovy algebry o 2^{2^n} prvcích (n je pevné celé kladné číslo). Uvedeme si zde šest Booleových vzájemně isomorfních, ale přesto vzájemně odlišných algeber, a to jak povahou svých prvků, tak způsobem realisace svazových úkonů, svazové jednotky a svazové nuly.

1. př.: *Prvky svazu*: Konečné části množiny (souboru) o 2^n předmětech.

Svazové spojení: Sjednocení částí. *Svazový průsek*: Průnik *Nula svazu*: prázdná část. *Jednotka svazu*: Celá množina.

2. př.: *Prvky*: Přirozená kladná čísla, dělitelé součinu 2^n prvních prvočísel

$$2 \cdot 3 \cdot 5 \cdot 7 \ldots p^{2^n} = N.$$

Svazové spojení: Nejmenší společný násobek. *Svazový průsek*: Největší společný dělitel. *Nula svazu*: Číslo 1. *Jednotka svazu*: Číslo N.

3. př.: *Prvky*: Vrcholky krychle v 2^n-rozměrném prostoru. *Svazové spojení*: K počátku nejbližší vrcholek, do něhož lze dojít po hranách krychle ze „spojovaných" vrcholků za neustálého vzdalování od počátku. *Svazový průsek*: Od počátku nejvzdálenější vrcholek, do něhož lze dojít po hranách krychle z obou „protínaných" vrcholků za neustálého přibližování se k počátku. *Nula svazu*: Vrcholek, ležící v počátku. *Jednotka svazu*: Vrcholek protilehlý k počátku (nejvzdálenější od počátku).

4. př: *Prvky*: Booleovské funkce o n nezávisle proměnných na Booleově algebře (0, 1). *Svazové spojení*: Funkce, jejíž hodnota je spojením hodnot daných funkcí (pro týž argument). *Svazový průsek*: Funkce, jejíž hodnota je průnikem hodnot daných funkcí. *Nula svazu*: Funkce s konstantní hod-

notou = 0. *Jednotka svazu*: Funkce s konstantní hodnotou = 1.

5. př.: *Prvky*: Elektrická *jj*-reléově-kontaktní zařízení o vstupních (řídících) klíčích (propouštějící nebo nepropouštějící proud jediným výstupem). *Svazové spojení*: Zařízení, sestrojené pomocí paralelního zapojení. *Svazový průsek*: Zařízení, sestrojené pomocí seriového zapojení (obou výstupních větví). *Svazová nula*: Zařízení, jež nikdy nepropouští proud. *Svazová jednotka*: Zařízení, jež vždy (za každé polohy řídicích kontaktů) převádí proud.

6. př.: *Prvky*: Výpovědi, které lze vyjádřit n jednoduchými, vzájemně nezávislými větami — při užití logických spojek „nikoli", „nebo", „a". *Svazové spojení* (dvou výpovědí): Je vyjádřeno spojením jejich větného vyjádření spojkou *nebo*. *Svazová nula*: Výpověď, vyjadřující logickou nemožnost. *Svazový průsek:* je vyjádřen spojkou *a*. *Svazová jednotka*: Výpověď, vyjadřující logickou samozřejmost (tautologii). (Pochopitelně, že toto nejsou všechny příklady možných Booleových algeber o 2^{2^n}prvcích. Př. 1 a 2 najde čtenář na obr. pro $n = 3$.)

Tím končíme více méně systematickou část našich výkladů o svazech. V dalším se věnujeme již jen nesystematickým doplňkům ve formě volné rozpravy, nečinící si nároků na matematickou přesnost.

Cvičení k 2,8.

1. Nalezněte logickou interpretaci všech 16 možných způsobů, jak tvořit složité výpovědi pomocí dvou daných výpovědí A a B a pomocí logických spojek $\vee$, &, $\sim$ („nikoli" („není pravda, že")). (Udejte si tabulky pro každou složenou výpověď.)

2. a) Převeďte každé logické souvětí složené ze dvou vět v souvětí, užívající jen logických spojek $\rightarrow$ a $\sim$.

b)*Vyjádřete všechna logická spojování vět pomocí jediné „spojky" „|" (Shefferův symbol), kde $A \mid B$ značí: nikoli A nebo nikoli B, algebraicky $A \mid B = A' \cup B'$.

3. Interpretujte de Morganovy identity jako (odvozené) poučky výrokové logiky.

4. Vztah (mezi výpověďmi) z A (logicky nutně) vyplývá B, je vztah částečného uspořádání v Booleově algebře výpovědí.

Ukažte, že říci, že z A logicky nutně vyplývá B (B je logický důsledek A) je totéž, jak říci, že výpověď $A \to B$ je jednotkou (příslušné Booleovy algebry výpovědí, je tautologickou výpovědí).

5. Říci, že A dává nutnou podmínku pro B značí $B \subseteq A$. Říci, že A dává nutnou a postačující podmínku pro B značí: $A = B$.

a) Odůvodněte následující, v matematice často užívaný postup důkazu nutnosti a postačitelnosti podmínky A pro B:

Existuje n výpovědí $C_1, C_2, \ldots, C_n$ tak, že $A = C_1$, $B = C_j$ (j pevné $1 < j < n$) z C_i plyne C_{i+1} pro $i = 1, 2, \ldots, n-1$ a z C_n plyne C_1 (t. zv. závěr pomocí implikačního kruhu).

b) Odůvodněte, že dokázat, že z A plyne B, je totéž, jako dokázat, že z $\sim B$ plyne $\sim A$.

c) Odůvodněte t. zv. nepřímý důkazový postup: dokázat, že z A plyne B, je totéž jako dokázat, že z předpokladu $\sim B \,\&\, A$ plyne kontradiktorická (sporná) výpověď.

2,9. MODULÁRNÍ SVAZY. MODULÁRNÍ A KOMPLEMENTÁRNÍ SVAZY. PROJEKTIVNÍ GEOMETRIE JAKO SVAZ. SPOJITĚ DIMENSIONÁLNÍ PROJEKTIVNÍ GEOMETRIE.

Jako v 1. části knížky (jednající o grupách) nám zbývá i zde k víceméně systematickým výkladům o základních pojmech a některých druzích svazů, jež tvoří hlavní obsah této druhé části, připojit nakonec zběžný pohled na některé další otázky a výsledky theorie svazů a jejich aplikací, na něž se tu nedostalo a ani nemohlo dostat. To je však úloha těžší, než v případě grup, jednak proto, že theorie svazů je (v daleko větší míře než dnes již vykrystalisovaná a dlouhým vývojem prošlá theorie grup) dosud ve stadiu počátečního rozvoje, v němž není ještě zcela jasno, jak půjde další vývoj a co z nedávných objevů si podrží trvalou cenu v matematice i v aplikacích. Za druhé je potíž v tom, že do hloubky jdoucí aplikace theorie svazů v ostatní matematice, o nichž by bylo záhodno zde informovat, vyžadují dosti značných znalostí a rozhledu v současné matematice, po př. matematické logice.

Tak zejména v abstraktní algebře představuje aplikace

theorie svazů formulaci jádra některých velmi obecných algebraických principů. Bez znalosti současné abstraktní algebry je tedy těžko o tom něco říci.

Proto omezíme náš pohled na další výsledky a pojmy z theorie svazů opravdu jen na několik málo ukázek, jež se dají alespoň naznačit bez dalších nároků na čtenářovy matematické vědomosti. Řekli jsme si již, ze základní axiomy theorie svazů 1′ až 5″ představují, jak se zdá, ještě příliš širokou a neucelenou základnu pro rozvíjení hlubší theorie. Základní axiomy je proto třeba ještě doplnit dalšími axiomy. To doplnění, které jsme provedli nejprve, totiž připojení obou axiomů distributivity, nás vedlo k t. zv. distributivním svazům. Byly to právě ty svazy, kde se svazové spojování a protínání dalo (v isomorfní representaci) vystihnout množinovým spojováním a množinovým protínáním (ve vhodném svazu množin čili v t. zv. množinovém okruhu). Připojení dalšího axiomu 7 (axiomu doplňku) jsme pak dostali t. zv. Booleovy algebry.

V mnoha často se vyskytujících typech svazů nejen, že není ani řeči o doplňku (ve smyslu axiomu 7), nýbrž i na místě obou axiomů distributivity je splněn jen jistý slabší, sám k sobě duální axiom, t. zv. axiom modularity, čili též axiom Dedekindův (nazvaný tak podle svého objevitele).

Ten zní takto:

Jsou-li a a c dva prvky svazu, splňující vztah $a \subseteq c$ (a jinak jsou libovolné), *pak pro libovolný prvek b platí rovnost*

$$a \cup (b \cap c) = (a \cup b) \cap c.$$

Smysl Dedekindova axiomu spočívá v jisté dosti abstraktně vyslovené podmínce „geometrické" pravidelnosti, jakou tento axiom ukládá svazovému částečnému uspořádání t. zv. modulárního svazu, ve kterém je splněn. Ukazuje se však, že Dedekindův axiom je logicky rovnocenný s dosti názorným požadavkem, aby se ve svazu nevyskytly nikdy tři různé prvky a, b, c tak, že by platilo $b \cap c \subset a \subset c \subset b \cup a$ (ve smyslu geometr. znázornění svazového částečného uspo-

řádání — bychom měli 5 bodů $a, b, c, a \cup b, b \cap c$) uspořádaných do pětiúhelníka jako na obr. 19, V). (Především se čtenář sám snadno přesvědčí, že by existence zmíněných tří prvků měla za následek $a = a \cup (b \cap c) \neq (a \cup b) \cap c = c$; čili: když platí axiom modularity, je výskyt zmíněných tří prvků jistě vyloučen. Obrácená souvislost, že totiž když je výskyt takových tří „nepravidelných" prvků vyloučen, pak že platí Dedekindův axiom, dá se rovněž snadno dokázat.

Rčením, že Dedekindův axiom je slabší, než každý z axiomů distributivity má být řečeno to, že z axiomu distributivity (jednoho nebo druhého) plyne axiom modularity (každý distributivní svaz je modulární), že však lze nalézt svazy, které nejsou distributivní a jsou nicméně modulární. První fakt je ihned vidět, neboť podle axiomu distributivity — třebas prvého 6′ (s druhým by se jen začalo s levé strany rovnosti v axiomu modularity místo s pravé) je vždy $(a \cup b) \cap c = (a \cup c) \cap (b \cup c)$. Následkem předpokladu $a \subseteq c$ je však $a \cap c = a$. Druhý fakt nahlédneme za pomoci obr. 19, IV podávajícího graf nejprostšího svazu, který je modulární — jak se čtenář sám snadným ověřením platnosti Dedekindova axiomu sám přesvědčí — ale není distributivní (což si čtenář rovněž snadno dokáže sám jako užitečné cvičení).

Modulární svazy se vyskytují dosti často v abstraktní algebře, jakožto *svazy podsystémů, obsažených v daném algebraickém systému.* Tak na př. všechny *normální podgrupy* libovolné dané grupy tvoří modulární (ale obecně nikoli distributivní) svaz, rozumíme-li spojení a průnik ve smyslu věty 9, (části 1.) (Avšak také samotné vhodné podsvazy daného svazu opět mohou tvořit modulární svaz.)

Za jistých předpokladů, o nichž se zde nelze šířit, se podgrupy v jistých komutativních (Abelových) grupách (kteréžto podgrupy jsou ovšem, jak víme, vždy normální) stávají tak zvanými *moduly.* Dedekindův axiom a jím objevený druh svazů má své druhé jméno podle toho, že jej Dedekind objevil ve svazu modulů. Ve všech těchto modulárních svazech moderní abstraktní algebry, prvky jsou jisté význačné podsystémy, obsažené v daném algebraickém systému (jako na př. normální podgrupy jsou takovými význačnými „podsystémy" v grupách, jestliže grupy považujeme za (poměrně prosté) algebraické systémy). Svazové polouspořádání je mezi „podsystémy" zde opět množinová inkluse, t. j. vztah „pod-

systém x je obsažen v podsystému y" (celého systému). Značí, že každý prvek patřící do x patří i do y. Je třeba však zdůraznit, že svazové spojování nikterak již není vždy množinovým sjednocováním, t. j. pouhým shrnováním prvků z daných dvou podsystémů do jednoho, protože takové pouhé shrnutí nepředstavuje už obecně podsystém daného systému.

Theorie svazů — a především modulárních svazů — představuje tedy nástroj, který pomáhá orientovat se ve výstavbě složitých algebraických systémů z jejich jednodušších význačných podsystémů — a v tom je její význam pro moderní algebraické theorie. Protože tedy aplikace theorie (modulárních) svazů na rozbor stavby složitých algebraických systémů nás poučuje o *struktuře* těchto systémů, proto bylo dáno svazům též jméno struktury. (Názvu struktura se užívá v ruštině, polštině a francouzštině.)

V tomto smyslu je dalekosáhlý zejména vztah mezi theorií modulárních svazů a theorii grup. Pro modulární svazy platí totiž tvrzení, která jsou vlastně svazovým vyjádřením (poněkud zeslabených) základních vět Jordan-Hölderovy a Remak-Schmidtovy a jiných vět o grupách (viz 1,8).

Zvláště dobře uzavřený a důležitý systém dodatkových axiomů (jimiž je třeba doplnit základní axiomy svazu) je kombinace Dedekindova *modulárního axiomu a axiomu 7 o doplňku*. Svazy, splňující kromě základních axiomů ještě axiom modularity a axiom doplňku jsou t. zv. modulární komplementární svazy. (Připomeňme hned, že zeslabením axiomů distributivity v axiom modularity přestává platit zásada, že k danému prvku je nutně třeba jen jednoho doplňku, jako je tomu v distributivních komplementárních svazech, t. j. v Booleových algebrách, viz str. 150.) Příklad takového svazu už známe z obr. 19, IV.

V abstraktní algebře se vyskytují takové modulární komplementární svazy, jakožto svazy význačných podsystémů algebraického systému. Tak na př. grupa, která se dá rozložit v direktní součin (viz str. 96 v 1,8) takových normálních svých podgrup, které jsou jednoduché (t. j. samy již nemají žádnou vlastní normální podgrupu), vytváří modulární komplementární svaz všech normálních podgrup.

Komplementární modulární svazy jsou však důležité především jako ten druh již zmíněných (viz str. 124 a str. 128)

svazů, jež zahrnují svazy dané *geometrickým protínáním a spojováním*, prováděným na přímkách, bodech, rovinách (a ve vícerozměrné geometrii na dalších vícerozměrných zobecněných přímek rovin). Tyto svazy ukazují v nejčistší formě zákonitosti geometrického protínání a spojování, jaké jsou studovány v projektivní geometrii.

Objasněme si alespoň v hrubých rysech, jakým způsobem je v rámci theorie modulárních komplementárních svazů axiomaticky založena t. zv. projektivní geometrie roviny.

V projektivní geometrii *roviny* (pojaté axiomaticky) nedefinujeme přímo, co je to bod a co je to přímka, nýbrž charakterisujeme tyto dva druhy pro nás základních geometrických útvarů jejich základními vlastnostmi a vzájemnými vztahy, t. zv. geometrickými axiomy (které samotné konec konců abstrahujeme z praxe, z názoru). Při tom se tyto základní vztahy opírají v projektivní geometrii především o neomezenou možnost *protínat* (přímky) a *spojovat* (body). (Projektivní geometrie nezná ani pojmu vzdálenosti bodů ani pojmu rovnoběžnosti přímek. Každé dvě přímky se mohou protnout.)

A tu se při axiomatickém zakládání projektivní geometrie ukazuje, že za projektivně geometrické axiomy lze prostě *považovat axiomy modulárního komplementárního svazu, doplněné* ještě o jeden jediný charakteristický axiom (jehož znění si uvedeme níže).

Je při tom ovšem třeba, jak již naznačeno, rozšířit pojem protínání dvou různých přímek a pojem spojování dvou různých bodů tak, aby pro jakékoli dva geometrické základní útvary byl bez jakýchkoli výhrad určen výsledek jejich spojení a jejich protnutí. Pak na př. axiomem 1′ můžeme zaručit geometrický axiom, že každé dva body lze spojit jedinou přímkou. Podobně axiom 1″ nám zaručuje, že každé dvě přímky se protnou v jediném bodě. Axiom 3′ říká, že spojit bod a s bodem b je totéž, jako spojit bod b s bodem a. Po-

dobně lze geometricky vyložit smysl ostatních axiomů svazu, což přenecháváme čtenáři. K tomu je jen zapotřebí doplnit přímky a body na jedné straně celou rovinou (v níž naše přímky a body leží) a na druhé straně onou nám již povědomou prázdnou částí roviny. Tato poslední bude patrně výsledkem „protětí" dvou různých bodů nebo přímky s bodem na ni neležícím a představuje nulu svazu. Celou rovinu je pak nutno pokládat za výsledek spojení dvou různých přímek nebo přímky s bodem, který na ni neleží; je to jednotka svazu. Svazovým polouspořádáním je pak (jak již víme z 2,3) geometrický vztah „X leží na Y". Svazovým *doplňkem* je k danému bodu každá přímka, která jím neprochází a k dané přímce každý bod, který na ni neleží. Zde je tedy ke každému prvku (s výjimkou celé roviny a její prázdné části) dokonce nekonečně mnoho doplňků — na rozdíl od Booleovy algebry. (Doplňkem celé roviny je ovšem její prázdná část a doplňkem prázdné části je celá rovina; při tom svazovou jednotkou je celá rovina sama, svazovou nulou prázdná část roviny.)

A nyní: Projektivní geometrii charakterisující axiom, který je třeba ještě připojit k axiomům modulárního komplementárního svazu, je právě ten, který tak ostře odlišuje geometrické svazy projektivního spojování a protínání od Booleových algeber (které jsou ovšem také (zvláštními) modulárními komplementárními svazy). Axiom zní takto — v geometrické řeči:

Ke každým dvěma různým bodům existuje přímka, na níž neleží ani jeden z nich.

Tento axiom (který tvrdí vlastně přímo opak zásady o jednoznačnosti doplňku v Booleově algebře) můžeme ovšem vysloviti v názvosloví theorie svazů, když si vzpomeneme na pojem *atomu* (který odpovídá *geometrickému* pojmu *bodu*) z odst. 2,5. (Tohoto pojmu tam bylo sice použito v případě konečné Booleovy algebry, ale byl zaveden zcela obecně, pro každý svaz s nulovým prvkem.)

Pak charakteristický axiom projektivní geometrie roviny zní:

Každé dva atomy mají společný doplněk.

Takto tedy, zběžně a bez důkazů načrtnuta, vypadá elementární projektivní geometrie roviny s hlediska theorie svazů. Souvisí tedy pojem modulárního a komplementárního svazu — po příslušném ohraničení od Booleovy algebry ještě uvedeným specifickým axiomem o existenci společných doplňků — úzce s našimi základními vědomostmi o prostoru, resp. o rovině, takže i touto cestou se svazy objevují ve svém bezprostředím vztahu ke skutečnosti. Připomeňme ještě již jednou zmíněnou okolnost, že t. zv. *princip duality projektivní geometrie* je takto převeden *na princip duality theorie modulárních komplementárních svazů*, na něž se základní princip duality theorie svazů rozšiřuje, následkem duální stavby jak axiomu modularity (který je duální sám k sobě) tak i axiomu doplňku (o němž platí totéž). Složitější pojmy projektivní geometrie, jako je na př. kolineace, dostávají ve svazovém pojetí elegantní formu. Tak kolineace se jeví jako isomorfní zobrazení svazu na sebe sama (čili jako t. zv. automorfismus).

(Vztah kolineace mezi přímkami a body projektivní roviny na př. je dán, jak je některým čtenářům známo, osou kolineace, t. j. pevnou přímkou a dvěma středy kolineace (mimo tuto přímku), t. j. dvěma pevnými body. Kolineace sama pak je vzájemně jednoznačné přiřazení bodů k bodům a přímek k přímkám (jejich obrazům), jež se sestrojuje za této zásady: osa kolineace odpovídá bod po bodu sama sobě. Středy kolineace si odpovídají vzájemně. Sestrojit bodu odpovídající bod (jeho kolineární obraz) znamená: daný bod spojit s jedním i druhým středem kolineace a do obou průsečíků těchto spojnic s osou kolineace vést spojnice z druhého a prvního středu kolineace. Pak průsečík těchto posledních dvou přímek je kolineární obraz daného bodu. Obraz přímky je pak již dán jako spojnice obrazů dvou bodů na ní.)

A nakonec ještě zmínku o jednom zvrcholných výsledků theorie svazů projektivní geometrie. Je to Von Neumannův[40] objev *projektivní geometrie se spojitě proměnnou dimensí.*

[40] Von Neumann je vynikající současný matematik a matematický fysik maďarsko rakouského původu.

Je dosti nesnadno i jen zhruba naznačit bez dalšího matematického aparátu, oč jde. Nicméně, pokusme se o to alespoň docela hrubým způsobem asi takto:

V běžné projektivní geometrii — mějme na mysli třeba projektivní geometrii prostoru — jsou (v běžném smyslu základní) geometrické útvary rozděleny do kategorií podle svého *rozměru* čili *dimense*. Tak body jsou útvary „bezrozměrnými" čili dimense 0, přímky jsou útvary jednorozměrnými čili dimense 1, rovina je dvoudimensionální základní geometrický útvar (dimense 2), prostor (v běžném smyslu slova) je dimense 3, a tak i dále (jdeme-li ke geometriím vícerozměrným). Při tom se svazovým spojováním geometrických útvarů dimense obecně zvětšuje (nebo alespoň nezmenšuje) a svazovým protínáním se zmenšuje (nezvětšuje). (Mohli bychom dokonce přesně říci kdy a jak, ale to by nás vedlo zbytečně daleko.) Tak na př. spojení dvou různých základních útvarů dimense 0, t. j. bodů — dostáváme útvar dimense 1 — přímku, spojení útvaru dimense 1 — přímky s útvarem dimense 0, bodem, dá rovinu, t. j. útvar dimense 2 (ale útvar dimense 2, t. j. rovinu, můžeme dostat i spojením tří různých útvarů dimense 0, t. j. tří bodů, atp.).

Ve spojitě dimensionální geometrii máme především také „základní geometrické útvary", totiž prvky jistého modulárního a komplementárního svazu, právě tak jako jsou body, přímky, roviny prvky modulárního komplementárního svazu projektivní geometrie. A můžeme říci, že tyto prvky tohoto svazu jsou opravdu zobecněním základních útvarů projektivní geometrie, bodů, přímek, rovin — protože modulární komplementární svazy, definující pojem spojitě dimensionální geometrie, splňují jisté další požadavky, jež jsou *přenesením onoho dodatkového axiomu, jímž jsme svaz projektivní geometrie roviny odlišili od Booleových algeber*. Také tyto abstraktní „geometrické útvary" jsou rozděleny do kategorií podobně, jako se základní útvary projektivní geometrie řadí do kategorií podle své dimense.

Avšak číslo, které základním útvarům spojitě dimensionální geometrie (t. j. prvkům uvažovaného svazu) je zapotřebí přiřadit jako jejich „dimensi", *může probíhat nyní i všechny reálné hodnoty mezi nulou a jednou.* A také zde se spojením (protínáním) dvou „základních geometrických útvarů" zvyšuje (snižuje) anebo alespoň nesnižuje (nezvyšuje) jejich „dimense". Ale rozkládáním útvaru ve spojení dvou útvarů nižší dimense nikdy nedojdeme k nejjednodušším, dále již takto nerozložitelným útvarům — t. j. k bodům: To znamená, že spojitě dimensionální projektivní geometrie *nemá bodů.*

Zdálo by se, že konstrukce spojitě dimensionální projektivní geometrie je abstraktní matematická hříčka (ostatně by snad bylo možno pochybovat o vhodnosti názvu „geometrie", pro jistý nekonečný modulární komplementární svaz, jehož prvky si nelze dobře názorně představit ač tento svaz splňuje stejné podmínky, jež splňují i názorně geometrické svazy). Avšak ukazuje se, že spojitě dimensionální projektivní geometrie se objevuje v těch partiích moderní matematiky, jež mají použití v *kvantové mechanice.* Nehledě na to, jak nečekaným způsobem theorie svazů objevem spojitě dimensionální geometrie zasáhla do našeho názoru na abstraktní jádro projektivní geometrie vůbec, máme tu tedy nový doklad pro to, že i velmi abstraktní a zdánlivě se skutečností nijak nesouvisící matematické theorie vždy mají, třebas nečekaný a nejprve neznámý, reálný význam.

2,10. ZÁVĚR DRUHÉ ČÁSTI KNÍŽKY.

Nakonec je třeba, abychom zrekapitulovali postup výkladu při svazech právě tak, jako jsme to učinili při grupách.

Vyšli jsme od velmi obecného a v podstatě každému dobře povědomého pojmu částečného uspořádání. U tohoto ve velmi rozmanitých tvarech se vyskytujícího pojmu jsme

poněkud prodleli pro jeho samostatnou důležitost. Definovali jsme také pojem polouspořádání, jakožto částečné uspořádání s připuštěním rovnosti; svaz jsme nejprve definovali jako polouspořádaný soubor (množinu), kde každé dva prvky mají (ve smyslu nějakého polouspořádání) svůj nejmenší společný „nadprvek" — čili t. zv. *spojení* a největší společný „podprvek" — čili t. zv. *průsek*. Ukázalo se však, že je právě tak dobře možno na svazy hledět podobně jako na grupy. To znamená, že lze považovat za základní nikoli pojem částečného uspořádání, resp. polouspořádání, nýbrž samo spojování a protínání jakožto „úkony", podrobené jistým axiomům, které dílem mají tutéž formu jako axiomy (komutativní) grupy, dílem jsou jiného rázu; pak svazem rozumíme každý soubor, v němž lze spojovat a protínat dle těchto axiomů. Charakteristické je na těchto axiomech svazu to, že se vyskytují ve dvojicích tak, že záměnou spojování za protínání a obráceně dostáváme z jednoho axiomu druhý (t. zv. *princip duality*).

Přenesli jsme dále z theorie grup i základní pojmy homomorfního a isomorfního zobrazení (svazu na svaz). (To jsou totiž vůbec obecné pojmy, vystupující v nejrůznějších specialisacích v abstraktní algebře.)

Uznavše, že základní axiomy svazu samy nestačí k charakterisaci důležitých druhů svazů, jež jsme poznali na příkladech, vybrali jsme ze známých doplňujících axiomů hlavně dva: *axiom distributivity* (a axiom k němu duální) a *axiom doplňku*. Svazy, které vedle základních axiomů splňují axiomy distributivity, jsou t. zv. *distributivní svazy*. Uvedli jsme, že jsou to právě ty svazy, kde svazové spojování a protínání se dá pomocí isomorfního zobrazení převést zcela na sjednocování a pronikání množin (t. zv. množinovou representací, jakožto zvláštním druhem realisace abstraktně daného typu svazu „konkretním" svazem množin čili množinovým okruhem — analogie k representaci „abstraktních" grup grupami permutací.)

V dalším jsme se omezili na distributivní svazy, splňující

axiom doplňku, čili na t. zv. *Booleovy algebry*; zde jsme pro případ konečných algeber větu o isomorfní množinové representaci podrobně dokázali.

Věnovali jsme se pak některým nejjednodušším aplikacím theorie konečných Booleových algeber, zejména algeber booleovských funkcí, a to na elektrotechniku (algebra reléově-kontaktních zařízení) a na matematickou logiku (algebra výpovědí ve smyslu výrokové logiky). Ukázala se na první pohled překvapující souvislost: obě tyto algebry jsou si isomorfní, jestliže počet vstupních klíčů m je roven počtu jednoduchých výpovědí — neboť v obojím případě jde — až na isomorfismus — o Booleovu algebru všech booleovských funkcí na algebře (0, 1) o m nezávisle proměnných.

Nakonec bylo přidáno několik zmínek o jiných důležitých druzích svazů, jež vycházejí z toho, že v nich místo axiomu distributivity platí slabší *axiom modularity*. Přidáme-li k axiomu modularity ještě axiom *doplňku* (při čemž nyní může být k jednomu prvku více různých doplňků) a dodáme-li ještě požadavek, že *dva různé prvky „téhož rozměru"* (na př. body) *mají vždy společný doplněk*, dostáváme svazovou charakterisaci geometrického spojování a protínání, jak je zná t. zv. *projektivní geometrie*. Zobecněním možno dospět k t. zv. spojitě-rozměrové projektivní geometrii, v níž není bodů a rozměry (dimense) základních geometrických útvarů se mění spojitě v intervalu mezi 0 a 1.

SEZNAM LITERATURY K DALŠÍMU STUDIU.

K theorii grup:

a) Učebnice:

A. G. Kuroš, *Těorija grup*, OGIZ Moskva 1944.
O. J. Šmidt, *Abstraktnaja těorija grup*, Kijev 1916, II. vyd. Moskva 1933.
A. Speiser, *Theorie der Gruppen endlicher Ordnung*, Springer, Berlin 1923, II. vyd. 1927.
H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Teubner, Lipsko 1937.
O. Borůvka, *Úvod do theorie grup*, JČMF Praha 1943.
Starší, ale stále ještě dobrá monografie:
W. Burnside, *Theory of groups of finite order*, Cambridge, University Press 1897.

b) Theorie representace a theorie charakterů:

D. E. Littlewood: *The Theory of Group Characters and Matrix Representations of groups*, Oxford 1940.

c) Aplikace na kristalografii:

J. J. Burckhardt, *Die Bewegungsgruppen der Kristallographie*, Basilej, Birkhauser 1947.

d) Aplikace na kvantovou mechaniku:

B. L. van der Waerden, *Die gruppentheoretische Methode in der Quantenmechanik*, Springer, Berlin 1932.

e) Aplikace na theorii rovnic (algebraických):

N. G. Čebotarev, *Těorija Galua*, Moskva.

f) Spojité grupy, aplikace na matematickou analysu:

L. S. Pontrjagin, *Něpreryvnyje grupy*, ONTI Moskva 1938.
N. G. Čebotarev, *Těorija grup Li*, GITL Moskva 1940.

K theorii svazů:

a) Učebnice: zatím neexistují. Místo toho monografie:

V. Glivenko, *Théorie des Structures*, Act. Sc. Ind., Paris 1938.
G. Birkhoff, *Lattice Theory*, Amer. Math. Soc. Coll. Publ. Vol. XXV, New York (včetně aplikací v matem.), 1. vyd. 1940, 2. rozš. vyd. 1948.
H. Hermes, G. Köthe, *Theorie der Verbände*, Enz. Math. Wiss., Band I_1, Heft 5.

b) Aplikace Booleových algeber na elektrotechniku:

Gavrilov, *Těorija relejno-kontaktnych schem*, Ak. Nauk SSSR, Moskva 1950.

Učebnice vyšší algebry, jichž studium by mělo doprovázet přečtení této knížky:

A. G. Kuroš: *Kurs vysšej algebry*, II. vyd., GITL Moskva 1949.

B. L. van der Waerden, *Moderne Algebra* I a II., 3. vyd., Springer, Vídeň 1950, 1951.

Ruský překlad: *Sovremennaja algebra*, Moskva 1947.

Svazky „Cesty", které souvisí bezprostředně s látkou této knížky:

Št. Schwarz: *O rovnicích.*

B. Pospíšil: *Nekonečno v matematice.*

Mir. Katětov: *Jaká je logická výstavba matematiky.*

O. Zich: *Úvod do filosofie matematiky.*

OBSAH.

Část 1. Theorie grup.

Část 2. Theorie svazů.

Cesta k vědění, sv. 65.

Dr Ladislav Rieger

O GRUPÁCH A SVAZECH

Vydalo Přírodovědecké vydavatelství, Praha 1952. — Šéfredaktor Ladislav Mach, odborný redaktor Miroslav Fuka, výtvarný redaktor Miloš Hrbas, jazyková redaktorka Věra Pašková. — Z nové sazby písmem Extended vytiskla Státní tiskárna n. p., závod 05 (Prometheus), Praha VIII. — 1. vydání, náklad 2750 výtisků (1—2750) — 301 03/2 — 127 — 1%. — Sazba 9. X. 1951, tisk 15. II. 1952 — 6,5 plánovacích archů, 11,17 autorských archů, 11,32 vydavatelských archů — 208 str., 26 obr. — Papír 222-17, formát 70 × 100, 80 g.

Cena brož. 96,— Kčs.

DT 512

CESTA K VĚDĚNÍ

svazek

65

Cena brož. Kčs 96,—

301 03/2
DT 512