4. Algebraické struktury

In: Herbert Kästner (author); Peter Göthner (author); Karel Horák (translator): Algebra, každý začátek je lehký. (Czech). Praha: Mladá fronta, 1986. pp. 126–161.

Persistent URL: http://dml.cz/dmlcz/404148

4. ALGEBRAICKÉ STRUKTURY

PŘED ZÁKONEM JSOU SI VŠICHNI ROVNI

4.1 GRUPY, OKRUHY A TĚLESA
Úvod a vysvětlení těchto pojmů

V odstavcích 3.1 až 3.3 jsme prozkoumali velký počet objektů, tj. množin s operacemi. Přitom jsme se především zajímali o vlastnosti operací v množině M. Neptali jsme se kupříkladu, zda M je konečná či nekonečná, neboť to nesouviselo s vlastnostmi operace definované v M. Ale ptali jsme se, zda je M vzhledem k dané operaci uzavřená, tj zda „součin" dvou prvků z M je opět prvek z M. Také nás v uvedené souvislosti málo zajímala konkrétní podstata prvků z M, ale spíš to, zda je mezi jejími prvky takový, jenž vzhledem k dané operaci hraje neutrální roli. Prohlédneme-li co nejvíce v matematice se vyskytujících objektů podle takovýchto typických vlastností, najdeme skupiny se společnými vlastnostmi, pro něž se zdá být vhodné jisté objekty s určitými vlastnostmi nějak pojmenovat. Přitom odhlédneme od konkrétní podstaty prvků množiny M stejně jako od konkrétní podstaty v M definované operace (operací). Zajímáme se jen o pravidla, kterými se operace v M řídí. Takový „seznam pravidel" definuje algebraickou strukturu. Budeme to hned teď ilustrovat na důležité algebraické struktuře „grupy". Každý konkrétní objekt pak buď splňuje podmínky daných zákonů grupy a je to (konkrétní) grupa, anebo souhrn podmínek, jež se také nazývají axiómy, nesplňuje a grupa to není.

V tomto smyslu slouží zavedení algebraických struktur především systemizaci matematického obsahu.

V následující tabulce je uvedeno 10 objektů, jež budeme zkoumat vůči čtyřem vlastnostem:

Množina M s binární operací $\circ$	M je uzavřená vzhledem k $\circ$	$\circ$ je asociativní	M obsahuje neutrální prvek vzhledem k $\circ$	Ke každému prvku z M existuje inverzní prvek vzhledem k $\circ$
$(\mathbf{Z}, +)$	p	p	p	p
$(\mathbf{Q} \setminus \{0\}, .)$	p	p	p	p
množina všech lichých čísel vzhledem ke sčítání v $\mathbf{Z}$	n	p (v $\mathbf{Z}$)	n	n
$(M_{(2,2)}, +)$	p	p	p	p
$(M_{(2,2)}, .)$	p	p	p	n
množina všech permutací množiny $\{1, \ldots, n\}$ vzhledem ke skládání	p	p	p	p
$(\mathbf{Z}/(4), +)$	p	p	p	p
$(\{(1)_{12}, (5)_{12}, (7)_{12}, (11)_{12}\},$ množina všech reálných funkcí vzhledem ke sčítání				
$(\{1, 2, 3, 6\}, \wedge)$				

Pro prvních sedm objektů je zaneseno „p“ či „n“ podle toho, zda výrok o vlastnosti uvažované operace je pravdivý nebo ne. Tak sčítání $+$ celých čísel je sice asociativní, ale množina lichých čísel není vůči $+$ uzavřená. Množina $M_{(2;2)}$ všech matic typu (2; 2) je uzavřená vzhledem k (asociativnímu) násobení a má i neutrální prvek $\mathbf{E}$, ale ne každý prvek této množiny má inverzní. Všechny objekty, u nichž v každém sloupci stojí znak p, dostanou společné jméno: říkáme, že jsou to příklady grupy, nebo stručně, že jsou to *grupy*. Vyplnění tří zbývajících řádků přenecháváme nyní čtenáři. Prozradíme, že se v naší tabulce vyskytuje právě sedm grup.

Definice 4.1. Neprázdná množina G s jednou binární operací $\circ$ se nazývá *grupa*, právě když splňuje následující axiómy:

$\mathbf{A}_1$: Pro všechna $a, b \in G$ platí také $a \circ b \in G$, tj. $\circ$ je neomezeně definovaná operace na G.

$\mathbf{A}_2$: Pro všechna $a, b, c \in G$ platí $(a \circ b) \circ c = a \circ (b \circ c)$, tj. $\circ$ je asociativní operace.

$\mathbf{A}_3$: V G existuje neutrální prvek e takový, že pro všechna $a \in G$ platí $a \circ e = e \circ a = a$.

$\mathbf{A}_4$: Ke každému prvku $a \in G$ existuje inverzní prvek $a^{-1} \in G$ takový, že platí $a \circ a^{-1} = a^{-1} \circ a = e$.

Objekty, v nichž jsou splněny jen axiómy $\mathbf{A}_1$ a $\mathbf{A}_2$, se nazývají *pologrupy*; mezi ně např. patří ($\{1, 2, 3, 6\}$, $\wedge$). Znak „$\circ$“ operace použitý v D(4.1) můžeme zřejmě interpretovat různě: jako znak pro násobení od nuly různých racionálních čísel, jako znak pro sčítání matic nebo znak pro skládání permutací.

Při popisu souvislostí v grupě zdomácněly v matematické literatuře dva způsoby, a sice multiplikativní způsob se znakem operace „$.$“ a aditivní způsob psaní

se znakem „+“. Obsah axiómů grupy přirozeně na zvoleném označení nezávisí.

Budeme dávat přednost multiplikativnímu způsobu psaní a také budeme používat pojmy „činitel“ a „součin“. Kromě toho však bude nutné používat i aditivní způsob psaní — především při charakterizaci množin, v nichž jsou definovány dvě operace. Pro grupu $(G, .)$ — pokud nebude hrozit nedorozumění — budeme také používat stručné označení G.

Vedle grup uvedených v tabulce najdeme množství dalších příkladů a protipříkladů, jestliže znovu projdeme množiny s operacemi uvedené v odstavcích 3.1 až 3.3. Tak např. množina všech reálných funkcí definovaných na intervalu $\langle a, b \rangle$ vzhledem ke sčítání funkcí a také množina všech posloupností reálných čísel vůči sčítání posloupností (srov. odstavec 3.1, příklad 4) jsou grupy. Tvoření aritmetického průměru v množině všech racionálních čísel naproti tomu není dokonce ani pologrupa, tím spíš to tedy není grupa (proč?). Pologrupami jsou objekty uvedené v příkladu 5, tedy např. $(\mathscr{P}(M), \bigcap)$.

Rozšíříme-li soustavu axiómů v D(4.1) o axióm $\mathbf{A}_5$: „Pro všechna $a, b \in G$ platí $a \circ b = b \circ a$“, mluvíme o komutativní grupě, nebo také (na počest norského matematika Nielse Henrika Abela[10])) o abelovské grupě. $(\mathbf{Z}, +)$ je abelovská, $(M_{(2,2)}, .)$ však ne. Grupa se nazývá *konečná* či *nekonečná* podle toho, zda množina, na níž je operace definována, je konečná či nekonečná. Počet prvků grupy nazýváme *řád grupy*. Mezi grupami uvedenými v naší tabulce je jedna řádu 4 (která?).

---

[10]) Niels Henrik Abel (1802—1829), norský matematik; už během svého studia se zabýval možností řešit algebraické rovnice 5. stupně pomocí radikálů (tj. hledal vzorce vyjadřující řešení takové rovnice). R. 1824 dokázal, že takové řešení pro libovolnou rovnici více než čtvrtého stupně není možné.

Objekty se dvěma operacemi, jako např. $(\mathbf{Z}, +, .)$, se často chovají vůči „sčítání" jako grupa, vůči „násobení" jako pologrupa. Je-li násobení navíc distributivně svázáno se sčítáním, mluvíme o okruhu.

Definice 4.2. Neprázdná množina R, v níž jsou neomezeně definovány dvě operace „$+$" a „$.$", se nazývá *okruh*, právě když jsou splněny následující axiómy:
$\mathbf{B}_1$: $(R, +)$ je komutativní grupa.
$\mathbf{B}_2$: $(R, .)$ je pologrupa.
$\mathbf{B}_3$: Pro všechna $a, b, c \in R$ platí

$$a.(b + c) = (a.b) + (a.c)$$

a

$$(b + c).a = (b.a) + (c.a).$$

Především je jasné, že symboly operací „$+$" a „$.$" použité v D(4.2) mohou být interpretovány různými způsoby; třeba jako sčítání a násobení v okruhu matic typu (n, n), jako sčítání a násobení v okruhu zbytkových tříd modulo 4 nebo jako sčítání a násobení v okruhu reálných funkcí. Naproti tomu $(\mathbf{N}_0, +, .)$ a $(\mathscr{P}(M), \cap, \cup)$ nejsou okruhy. Použijeme-li v $\mathbf{B}_3$ úmluvu, že „$.$" spojuje silněji než „$+$", mohou odpadnout závorky na pravé straně obou rovností.

Zřejmě každý okruh obsahuje neutrální prvek o vůči sčítání, neobsahuje však nutně podobný prvek vůči násobení, jak ukazuje okruh sudých čísel. Tuto asymetrii okruhu, jež byla zdůrazněna už v axiómech $\mathbf{B}_1$ a $\mathbf{B}_2$, můžeme odstranit, budeme-li vyžadovat vlastnosti grupy i pro multiplikativní operaci:

Definice 4.3. Množina K s alespoň dvěma prvky, v níž jsou dány dvě neomezeně definované operace, se nazývá *těleso*, právě když jsou splněny následující axiómy:
$\mathbf{B}_1^*$: $(K, +)$ je komutativní grupa.
$\mathbf{B}_2^*$: $(K \setminus \{o\}, .)$ je komutativní grupa.

$\mathbf{B}_3^*$: Pro všechna $a, b, c \in K$ platí

$$a.(b + c) = a.b + a.c.$$

Porovnáme D(4.3) s D(4.2). $\mathbf{B}_1^*$ souhlasí — až na označení množin — s $\mathbf{B}_1$. Násobení je sice definováno pro všechny prvky K, $\mathbf{B}_2^*$ však vyžaduje splnění všech axiómů grupy, zejména existenci inverzního prvku, jen pro prvky různé od o. Kdyby se nyní K skládalo jen z jednoho prvku (to by pak musel být neutrální prvek o), bylo by $K \setminus \{o\}$ prázdné. Konečně z $\mathbf{B}_3^*$ spolu s komutativitou „.“ plyne výrok $\mathbf{B}_3$.

Zřejmě je každé těleso také okruh, ale ne obráceně. $(\mathsf{Q}, +, .)$, $(\mathsf{R}, +, .)$ a $(\mathsf{Z}/(7), +, .)$ jsou příklady těles. Obecně je $(\mathsf{Z}/(n), +, .)$ jen okruh, tzv. *okruh zbytkových tříd modulo n*; je to těleso, právě když n je prvočíslo. Omezíme-li množinu zbytkových tříd jen na tzv. nesoudělné zbytkové třídy modulo n — to jsou ty zbytkové třídy, jejichž reprezentanti jsou nesoudělní s modulem n — , tak sice dostaneme vzhledem k násobení grupu, grupu nesoudělených zbytkových tříd modulo n (srov. tabulku na str. 118 pro $n = 12$), ale ztratíme vlastnosti grupy vzhledem ke sčítání.

Vytvoření takových pojmů jako grupa, okruh nebo těleso je výsledkem dlouhého historického vývoje matematiky a děje se abstrakcí, tj. odvržením speciálních vlastností rozličných objektů a formulováním společných vlastností. Plodnost a význam těchto pojmů spočívá v tom, že jsou na jedné straně dostatečně obecné, aby dovolily rozsáhlé aplikace na konkrétní objekty, a na druhé straně jsou definovány pomocí dostatečně přísného „seznamu pravidel“, jenž umožňuje rozsáhlé obecné závěry, výstavbu celé matematické teorie pouze z axiómů. Kupříkladu teorii grup dnes s velkým úspěchem používají fyzikové, krystalografové a další přírodovědci.

4.2 JEDNODUCHÉ DŮSLEDKY AXIOMATICKÝCH SYSTÉMŮ

Čtenář se důvěrně seznámí s důsledky axiómů grupy, okruhu a tělesa. Ukáže se, že strukturně teoretické úvahy mohou poskytnout kromobyčejně úsporné důkazy

Pěkný výkon, který vykonal malý udatný krejčík: jednou ranou zabil sedm much. My ho můžeme snadno předčit: „jedinou ranou" dokážeme výroky o vlastnostech všech grup; skrovný systém axiómů a inteligence budou přitom naše jediné zbraně. Získáme tedy znalosti i o sedmi grupách zahrnutých do tabulky v odstavci 4.1, aniž bychom tyto objekty museli jednotlivě vyšetřovat.

Zacházení se strukturami dovoluje vedle systemizace matematického obsahu postupovat úsporně při důkazech jednotlivých výroků, což hned ukážeme na několika příkladech.

V axiómu grupy $\mathbf{A}_3$, resp. $\mathbf{A}_4$ se požaduje, aby v každé grupě byl alespoň jeden neutrální prvek e, resp. aby ke každému prvku a grupy existoval alespoň jeden inverzní prvek a^{-1}. Otázku, zda v grupě může být případně i více neutrálních prvků, můžeme okamžitě zodpovědět záporně, když si uvědomíme důkaz zformulovaný v odstavci 3.3: Abychom mohli ze vztahů $e_1.e_2 = e_1$ a $e_1.e_2 = e_2$ dostat vztah $e_1 = e_2$, k tomu jistě nepotřebujeme žádné další vlastnosti operace „.", kromě těch, které jsou obsaženy v axiómech grupy.

Předpokládáme-li, že v grupě existují k prvku a dva různé inverzní prvky a^{-1} a a^*, vedou rovnosti $a^{-1} = a^{-1}.e = a^{-1}.(a.a^*) = (a^{-1}.a).a^* = e.a^* = a^*$ ke sporu $a^{-1} = a^*$. Odtud ve spojení s $\mathbf{A}_4$ plyne, že v každé grupě ke každému prvku existuje právě jeden inverzní prvek. Můžeme tedy shrnout:

Věta 4.1. *V každé grupě* $(G, .)$ *existuje právě jeden neutrální prvek* e *a ke každému prvku* a *existuje právě jeden inverzní prvek* a^{-1}.

Zřejmě nemůže být slovo „grupa" ve V(4.1) nahrazeno slovem „pologrupa", neboť ani existence neutrálního prvku e ještě nezaručuje existenci inverzního prvku a^{-1} k libovolnému prvku a pologrupy. V důkazu jednoznačnosti neutrálního prvku se však nepoužilo nic víc z vlastností operace než to, co je k dispozici z axiómů pologrupy; tj. existuje-li v pologrupě neutrální prvek, pak existuje nejvýše jeden.

Obsahuje-li nyní pologrupa neutrální prvek e, mohou se předchozí úvahy použít také pro prvky pologrupy. Oba důkazy tedy dovolují důsledek: *V pologrupě existuje nejvýše jeden neutrální prvek, a jestliže existuje, má každý prvek pologrupy nejvýše jeden inverzní prvek.*

Jednoznačně určený neutrální prvek grupy bývá při multiplikativním způsobu psaní označován jako e, při aditivním způsobu jako o a nazývá se — jak bylo už uvedeno v odstavci 3.3 —, *jednotkový* anebo *nulový prvek*. Analogicky se při aditivním značení píše $-a$ místo a^{-1} a mluví se o prvku *opačném* k a.

V množinách, v nichž jsou zavedeny operace, se obvykle provádějí výpočty. Budeme zkoumat, jaká početní pravidla se dají v grupě používat. Uvažujme nejprve zda a jak můžeme v grupě řešit lineární rovnici $a.x = b$. Díky $\mathbf{A}_3$ leží v G spolu s a a b i a^{-1} a díky $\mathbf{A}_1$ i $a^{-1}.b$. Posledně uvedený prvek je však řešením rovnice $a.x = b$, neboť platí

$$a.(a^{-1}.b) = (a.a^{-1}).b = e.b = b.$$

Má tedy každá rovnice $a.x = b$ alespoň jedno řešení. Bylo by potěšující, kdyby každá taková rovnice byla dokonce řešitelná jednoznačně. To dostaneme snadno

z následující úvahy: Předpokládejme, že x_1 a x_2 jsou dvě různá řešení rovnice $a.x = b$; tj. že platí jak $a.x_1 = b$, tak i $a.x_2 = b$. Z rovnosti pravých stran plyne i rovnost levých stran, tedy $ax_1 = ax_2$. Dále dostáváme $a^{-1}.(a.x_1) = a^{-1}.(a.x_2)$ a $(a^{-1}.a).x_1 = (a^{-1}.a).x_2$, a konečně $e.x_1 = e.x_2$, tudíž $x_1 = x_2$ ve sporu s předpokladem. Poslední část důkazu ukazuje, že grupová operace má vlastnost krácení.

Věta 4.2. *V grupě má každá rovnice tvaru* $a.x = b$, *resp.* $y.a = b$ *právě jedno řešení* $x = a^{-1}.b$, resp. $y = b.a^{-1}$.

Důkaz, že každá rovnice $y.a = b$ je jednoznačně řešitelná, přenecháváme čtenáři. Kromě toho si rozmyslete, proč nemůžeme takovou větu formulovat pro pologrupu!

Jiný výklad věty V(4.2) by byl: grupová operace je jednoznačně invertibilní.

Přesvědčme se, zda už nepřinesla ovoce lákavá myšlenka nahradit množství jednotlivých zkoumání využitím axiómů grupy: Jestliže jsme v úvodních příkladech (tabulka v odstavci 4.1) pátrali po neutrálních prvcích, teď víme: v sedmi grupách existuje právě jeden neutrální prvek, v každé ze tří pologrup se může vyskytovat nejvýše jeden neutrální prvek. Uveďte neutrální prvky a sestrojte pologrupu, která nemá neutrální prvek!

V(4.2) zahrnuje výrok, že pro čtvercové n-řádkové matice $\mathbf{A}$, $\mathbf{B}$ je každá maticová rovnice $\mathbf{A} + \mathbf{X} = \mathbf{B}$ jednoznačně řešitelná, ne nutně však každá maticová rovnice $\mathbf{A}.\mathbf{X} = \mathbf{B}$. Naproti tomu jsou jednoznačně řešitelné rovnice $(a)_4 + (x)_4 = (b)_4$, $(y)_7.(a)_7 = (b)_7$ a $(a_n) \oplus (x_n) = (b_n)$. Řešení lze bezprostředně uvést.

Také bychom mohli nadhodit otázku, proč užívat k definici pojmu grupy právě ty požadavky obsažené v axiómech $\mathbf{A}_1$ až $\mathbf{A}_4$, případně zda by se k charakteriza-

ci pojmu grupy nehodily i jiné vlastnosti. Můžeme dokázat následující větu:

Věta 4.3. *Objekt* $(G, .)$ *je grupa, právě když jsou splněny následující podmínky:*
$\mathbf{A}_1$: *Pro všechna* $a, b \in G$ *platí také* $a.b \in G$.
$\mathbf{A}_2$: *Pro všechna* $a, b, c \in G$ *platí* $(a.b).c = a.(b.c)$.
A: *Pro všechna* $a, b \in G$ *existují prvky* $x \in G$ *a* $y \in G$ *takové, že* $a.x = b$ a $y.a = b$.

V(4.3) říká, že výroky $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ a $\mathbf{A}_4$ jsou logicky ekvivalentní výrokům $\mathbf{A}_1$, $\mathbf{A}_2$ a **A**. Dají se tedy také tyto tři posledně jmenované výroky využít k charakterizaci pojmu grupy pomocí soustavy výroků. Důkaz V(4.3) dostaneme ve dvou krocích (a) a (b):
(a): Z $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ a $\mathbf{A}_4$ plyne $\mathbf{A}_1$, $\mathbf{A}_2$ a **A**.
Zřejmě stačí ukázat, že **A** vyplývá z $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$. **A** je oslabená formulace V(4.2), **A** tedy plyne bezprostředně z této věty. V(4.2) sama ale byla dokázána použitím $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ a $\mathbf{A}_4$.
(b): Protože z $\mathbf{A}_1$, $\mathbf{A}_2$ a **A** jistě plyne $\mathbf{A}_1$ a $\mathbf{A}_2$, postačí dokázat výroky $\mathbf{A}_3$ a $\mathbf{A}_4$.
Nejprve provedeme o něco obtížnější důkaz $\mathbf{A}_3$: Nechť a je libovolný (ale pevně zvolený) prvek G. Díky **A** má rovnice $a.x = a$ alespoň jedno řešení, nechť je to e_P. Platí tedy $a.e_P = a$. Jestliže má být e_P pravý neutrální prvek, musí splňovat každou rovnici tvaru $b.x = b$ pro libovolné $b \in G$. Abychom získali vztah mezi b a pevně zvoleným a, uvažujme pomocnou rovnici $y.a = b$, která má řešení c, tj. platí $c.a = b$. Nyní máme

$$b.e_P = (c.a).e_P = c.(a.e_P) = c.a = b.$$

Analogickou úvahou dostaneme, že také existuje alespoň jeden prvek $e_L \in G$ takový, že $e_L.b = b$ platí pro

všechna $b \in G$. Ještě zbývá ukázat, že každý levý neutrální prvek e_L je totožný s každým pravým neutrálním prvkem e_R. To dostaneme hned ze vztahu

$$e_L.e_P = e_L \quad \text{a} \quad e_L.e_P = e_P \text{ (srov. odstavec 3.3).}$$

Důkaz $\mathbf{A}_4$ není obtížný: Nechť a_P^{-1} je řešení rovnice $a.x = e$ a a_L^{-1} řešení rovnice $y.a = e$ pro libovolné $a \in G$, pak je

$$a_L^{-1} = a_L^{-1}.e = a_L^{-1}.(a.a_P^{-1}) =$$
$$= (a_L^{-1}.a).a_P^{-1} = e.a_P^{-1} = a_P^{-1}.$$

Existuje tedy ke každému $a \in G$ prvek a^{-1}, přičemž $a^{-1}.a = a.a^{-1} = e$.

Prozkoumáme nyní souvislost mezi grupami a pologrupami. Má-li operace v pologrupě H vlastnost krácení, nazývá se H *regulární pologrupa*. Přirozeně je každá grupa speciálně pologrupa a v důkazu V(4.2) jsme dostali, že grupová operace má vždy vlastnost krácení. Platí tudíž následující věta:

Věta 4.4. *Každá grupa je regulární pologrupa.*

Tato věta je ovšem málo vzrušující; zajímavá je však otázka, zda také platí obrácení věty V(4.4). Kdyby tomu tak bylo, musely by axiómy grupy plynout z axiómů pologrupy a z vlastnosti krácení. Přes intenzívní snažení se nám takový důkaz asi nepodaří, takže bychom se mohli domnívat, že obrácení věty V(4.4) neplatí, tj. že ne každá regulární pologrupa je grupa. Abychom toto ukázali, stačilo by dát příklad jedné regulární pologrupy, která (ještě) není grupa. $(\mathsf{N}_0, +)$ je vhodným příkladem: z $a + c = b + c$ vždy plyne $a = b$ pro všechna a, b, $c \in \mathsf{N}_0$ a $(\mathsf{N}_0, +)$ je pologrupa, ale nikoli grupa. Zostříme-li však předpoklady přijetím podmínky, že množina

všech prvků pologrupy je konečná, dají se už vlastnosti grupy dokázat, tj. platí věta:

Věta 4.5. *Každá konečná regulární pologrupa je grupa.*

Důkaz přenecháváme čtenáři (srov. cvičení 5a).

Sledujme náš cíl najít pravidla pro počítání v grupách dále: Tvrdíme, že pro libovolné prvky a, b grupy platí $(a.b)^{-1} = b^{-1}.a^{-1}$. Podle definice inverzního prvku k $a.b$ je $(a.b)^{-1}$ řešením rovnice $(a.b).x = e$. Na druhé straně řeší tuto rovnici i $b^{-1}.a^{-1}$, jak snadno zjistíme dosazením. Tvrzení bezprostředně plyne z jednoznačnosti řešení lineárních rovnic v grupě uvedené ve V(4.2).

Právě tak se dokáže $(a^{-1})^{-1} = a$, neboť jak a, tak $(a^{-1})^{-1}$ řeší rovnici $a^{-1}.x = e$ (návod: $(a^{-1})^{-1}$ je podle definice inverzní prvek k a^{-1}).

Stejně jako při násobení čísel, dá se zavést pojem n-té mocniny i pro grupovou operaci a místo součinu n stejných činitelů a psát a^n. Mocniny prvků grupy definujeme pro celočíselné exponenty n.

Definice 4.4. Pro každý prvek a grupy $(G, .)$ a pro každé celé nezáporné číslo k klademe:

(1) $a^0 = e$, (2) $a^{k+1} = a^k.a$, (3) $a^{-k} = (a^k)^{-1}$,

a^k se nazývá *k-tá mocnina prvku a.*

Z D(4.4), z (1) a (2) bezprostředně plyne $a^1 = a^{0+1} = a^0.a = e.a = a$. Jako při počítání s mocninami čísel, platí i v grupě pravidla $a^n.a^m = a^{n+m}$ a $(a^n)^m = a^{nm}$ pro libovolné $a \in G$ a celočíselné exponenty m a n. Naproti tomu vztah $(a.b)^n = a^n.b^n$ známý z počítání s čísly platí jen v abelovských grupách.

Pro přirozená čísla m a n vyjde důkaz matematickou

indukcí tak jako pro $a^1 = a$ použitím D(4.4), (1) a (2).

Až dosud a^{-1} označovalo inverzní prvek k a, tedy žádnou mocninu; vztah (3) ukazuje, že mocnina a s exponentem -1 je totožná s inverzním prvkem k a.

D(4.4) byla založena na multiplikativním způsobu psaní grupové operace. Přeneseme-li tuto definici na aditivní způsob psaní, odpovídá součinu $a.a. \ldots .a$ n stejných činitelů a součet $a + a + \ldots + a$ n stejných sčítanců a píšeme $n.a$. D(4.4) pak přejde v definici: Pro každý prvek a grupy $(G, +)$ a každé celé nezáporné číslo k klademe:

$$(1)\ 0.a = o,\quad (2)\ (k+1).a = k.a + a,\quad (3)\ (-k).a = k.(-a).$$

Stejným způsobem se dají „přeložit" důsledky D(4.4) do aditivního způsobu psaní, např. rovnost $a^n.b^n = (a.b)^n$ přejde v rovnost $n.a + n.b = n.(a + b)$. Tento přechod může nezkušenému čtenáři způsobit těžkosti, pokud nepozná, že $n.a$ je zkrácený zápis pro $a + a + \ldots + a$, a ne třeba dodatečně zavedené „násobení" v aditivní grupě; vždyť přirozené číslo n obecně ani není prvkem dané grupy.

Konečné objekty můžeme popsat tabulkou operace. Snadno si namalujete tabulku „sčítání" čtyř barev — červené, žluté, bílé a modré. Není těžké vidět, že přitom nemáme před sebou grupu, protože množina $\{č, ž, b, m\}$ není uzavřená vůči uvedenému sčítání.

Abychom zjistili, do jaké míry se dají vlastnosti grupy vyčíst z tabulky operace, podívejme se na příklad algebraické struktury $(\{e, a, b, c\}, .)$. Protože na každém místě tabulky stojí jeden z prvků množiny M, je splněn axióm $\mathbf{A}_1$. Axióm $\mathbf{A}_3$ se odráží ve skutečnosti, že alespoň jeden řádek a jeden sloupec tabulky se neliší od úvodního řádku (sloupce).

.	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

.	u	v	w	x	y	z
u	u	v	w	x	y	z
v	v	w	u	y	x	z
w	w	u	v	z	x	y
x	x	y	z	w	v	u
y	y	z	x	v	u	w
z	z	x	y	u	v	w

Protože v každém řádku a v každém sloupci tabulky se vyskytuje alespoň jednou neutrální prvek e, splňuje $(M, .)$ i $\mathbf{A}_4$. Platnost $\mathbf{A}_2$ (asociativita operace) se dá z tabulky stěží zjistit jednodušeji, než že se podvolíme pracné úloze vypsat všechna možná uzávorkování tří prvků a porovnat vypočítané součiny. V případě operace určené tabulkou 1 to vede k úspěchu, tj. $(M, .)$ je grupa. Ze sousední tabulky 2 zjistíme sice, že $\mathbf{A}_1$, $\mathbf{A}_3$ a $\mathbf{A}_4$ jsou splněny, $\mathbf{A}_2$ však pro tuto operaci neplatí, neboť $(y.x).w = u$, ale $y.(x.w) = w$. Není tedy $(\{u, v, w, x, y, z\}, .)$ grupa, a dokonce ani pologrupa.

Příklad navíc ukazuje, že $\mathbf{A}_2$ je na axiómech $\mathbf{A}_1$, $\mathbf{A}_3$ a $\mathbf{A}_4$ nezávislý. Pologrupa s neutrálním prvkem, která není grupa, jako např. $(\mathsf{N}_0, +)$, ukazuje, že z axiómů $\mathbf{A}_1$, $\mathbf{A}_2$ a $\mathbf{A}_3$ neplyne $\mathbf{A}_4$. Kdyby se dal některý axióm — třeba $\mathbf{A}_2$ — odvodit z ostatních axiómů grupy, tak bychom ho mohli v dané soustavě axiómů v D(4.1) škrtnout, nebyl by pro charakterizaci grupy vůbec nutný. Obecně se pro definici struktury volí minimální systém axiómů, nepoužíváme tedy pokud možno výroky, jež by se po důkladnějším rozmyšlení daly odvodit z ostatních. Vedle těchto spíš estetických požadavků na nezávislost jednotlivých výroků systému axiómů přirozeně musejí být tyto výroky bezesporné a postačovat k popisu dané struktury, o níž máme přesnou představu (úplnost axiomatického systému).

Komutativita operace (axióm $\mathbf{A}_5$) se snadno pozná

ze symetrie tabulky. Přirozeně i důsledky axiómů grupy mohou býti zřetelné z tabulky: To, že se v každém řádku a v každém sloupci tabulky vyskytuje každý prvek aspoň jednou, je právě výrok **A**.

Napišme mocniny prvků grupy charakterizované tabulkou 1:

$$\ldots, e^{-3} = e, e^{-2} = e, e^{-1} = e, e^0 = \\ = e, e^1 = e, e^2 = e, e^3 = e, \ldots$$
$$\ldots, a^{-3} = a, a^{-2} = b, a^{-1} = c, a^0 = \\ = e, a^1 = a, a^2 = b, a^3 = c, \ldots$$
$$\ldots, b^{-3} = b, b^{-2} = e, b^{-1} = b, b^0 = \\ = e, b^1 = b, b^2 = e, b^3 = b, \ldots$$
$$\ldots, c^{-3} = c, c^{-2} = b, c^{-1} = a, c^0 = \\ = e, c^1 = c, c^2 = b, c^3 = a, \ldots$$

Zřejmě nepotřebujeme pokračovat v tomto výčtu ani nalevo, ani napravo, neboť prvky se opakují v cyklu charakteristickém pro každý prvek grupy. Zatímco platí $e^n = e$ pro každé $n \in \mathsf{N}_0$ a už druhá mocnina b dává zas neutrální prvek e, dostaneme ze čtyř prvních mocnin a, resp. c všechny prvky grupy; $n = 4$ je nejmenší kladný exponent, pro nějž platí $a^n = e$, resp. $c^n = e$. Říkáme, že každý z obou prvků může „vytvořit" celou grupu.

Definice 4.5. Objekt $(M, .)$ se nazývá *cyklická grupa*, právě když platí:
(1) $(M, .)$ je grupa.
(2) M může být vytvořena jedním prvkem $a \in M$, tj. v M existuje takový prvek a, jehož mocniny a^n pro $n \in \mathsf{Z}$ tvoří všechny prvky grupy.

Prvek a se nazývá *vytvořující**) *prvek* (nebo také *generá-*

*) Používané, ale gramaticky nesprávně tvořené přídavné jméno. Správně by mělo být *vytvářející*... (Pozn. red.)

tor) grupy $(M, .)$, symbolicky to budeme zapisovat jako $M = \langle a \rangle$.

V našem úvodním příkladu jsou a a c vytvořující prvky, naproti tomu e a b „vytvářejí" jen vlastní podmnožinu M, jež však sama splňuje axiómy grupy vzhledem k operaci definované na celé grupě.

Pro každý prvek x naší konečné grupy existuje tedy nejmenší kladný exponent n takový, že $x^n = e$; toto číslo nazýváme *řád prvku*. Má tedy e řád 1, b řád 2 a a a c řád 4.

Uvažujme množinu čísel

$$\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots$$

vzhledem k operaci násobení. Protože se každý prvek dá vyjádřit jako mocnina 2 a všechny prvky jsou různé, sestrojili jsme příklad nekonečné cyklické grupy, jejímž vytvořujícím prvkem je 2.

Chceme-li najít další příklady cyklických grup, musíme se v grupách porozhlédnout po vytvořujících prvcích. V grupě zbytkových tříd modulo 7 je takovým prvkem jak $(3)_7$, tak i $(5)_7$. Grupa $(\{1, -1, i, -i\}, .)$ může být vytvořena jak prvkem i, tak i prvkem $-i$.

Aditivní grupa celých čísel jako vytvořující prvky obsahuje čísla $+1$ a -1, aditivní grupa zbytkových tříd modulu m prvky $(1)_m$ a $(m - 1)_m$.

Naproti tomu $(R \setminus \{0\}, .)$ a grupa s prvky $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$ se skládáním funkcí jakožto operací nejsou cyklické. U druhého příkladu to poznáme hned: každý prvek je sám k sobě inverzní, nemůže tedy vytvořit celou grupu. Abychom odůvodnili první příklad, musíme ještě trochu pokročit.

Cyklická grupa G je vždy abelovská. Jsou-li totiž b a c libovolné prvky G, mohou být oba vyjádřeny jako mocniny vytvořujícího prvku a, odkud plyne:

$$b.c = a^n.a^m = a^{n+m} = a^{m+n} = a^m.a^n = c.b.$$

Existuje velká rozmanitost grup se zcela rozdílnou „stavbou". Struktura cyklických grup je naproti tomu snadno přehledná. Zřejmě každá grupa G je buď konečná, nebo nekonečná. Je-li nadto G cyklická s vytvořujícím prvkem a, dají se oba tyto případy studovat blíže: V prvním případě (G konečná cyklická grupa) jistě nemohou být všechny mocniny a^n s celočíselným n různé, neboť by to odporovalo konečnosti G. Existují tedy různé exponenty h, k (přitom nechť $h > k$), pro něž $a^h = a^k$. Odtud podle pravidel pro mocnění plyne $a^{h-k} = a^l = e$; existuje tudíž alespoň jeden kladný exponent $l = h - k > 0$, pro nějž $a^l = e$. Mezi všemi kladnými exponenty s touto vlastností označme nejmenší jako t. Pak jsou $a^0 = e$, $a^1 = a$, a^2, a^3, ..., a^{t-1} všechny prvky G. Především jsou všechny uvedené mocniny navzájem různé; jinak by totiž nebylo t nejmenší kladný exponent s vlastností $a^t = e$. Každá mocnina a^n s celočíselným n se ale už vyskytuje mezi prvními t mocninami, neboť použijeme-li na n a t dělení se zbytkem $n = qt + r$, $0 \leqq r < t$, dostaneme $a^n = a^{qt+r} = (a^t)^q.a^r = e^q.a^r = a^r$, kde $0 \leqq r < t$. Počítání v této grupě G se pak redukuje na počítání s mocninami a^0, a^1, ..., a^{t-1} vytvořujícího prvku a; vyskytne-li se přitom exponent $n \geqq t$, můžeme ho, jak jsme už ukázali, redukovat prostřednictvím vztahu $a^t = e$. Násobení v G se tedy děje sčítáním exponentů jako v grupě zbytkových tříd modulo t. Výsledek: Píšeme-li prvky konečné cyklické grupy G jako mocniny vytvořujícího prvku a ve tvaru a^0, a^1, a^2, ..., a^{t-1}, provádí se násobení v G prostřednictvím sčítání exponentů modulo t.

Druhý případ (G nekonečná cyklická grupa) je ještě jednodušší. Zde musejí být všechny mocniny a^n (n celé číslo) navzájem různé, protože rovnost dvou takových mocnin s různými exponenty vede na konečnost G (srov. 1. případ). Pak dávají mocniny $\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a^1 = a, a^2, a^3, \ldots$ všechny prvky G a násobení v G se provádí sčítáním exponentů, tj. jako v aditivní grupě celých čísel. Tato situace nám prozrazuje: Každá nekonečná cyklická grupa má zřejmě stejnou „strukturu" jako aditivní grupa Z celých čísel a každá konečná cyklická grupa řádu n má stejnou „strukturu" jako aditivní grupa $\mathsf{Z}/(n)$ zbytkových tříd modulo n.

Speciálně odtud plyne, že $(\mathsf{R} \setminus \{0\}, .)$ nemůže být cyklická, protože jinak by musela tato grupa mít stejnou strukturu jako Z. To však mít nemůže, neboť ani není možné najít vzájemně jednoznačné zobrazení Z na R, protože Z je spočetná, zatímco R má mohutnost kontinua.

Prozkoumáním stavby cyklických grup končí náš výlet k počátkům teorie grup.

Princip vytváření důsledků z axiómů struktury je přirozeně možno použít i na okruhy a tělesa. Nejdříve bychom chtěli přenést na tyto struktury některé už získané znalosti:

Každý okruh a tím spíš každé těleso má právě jeden nulový prvek. Ne každý okruh — těleso však ano — má právě jeden jednotkový prvek. Obsahuje-li okruh jednotkový prvek, obsahuje takový prvek právě jeden. V každém tělese je jednoznačně řešitelná jak každá rovnice $a + x = b$, tak i každá rovnice $c.y = d$ $(c \neq o)$; v okruhu je obecně jednoznačně řešitelná jen rovnice $a + x = b$.

Použijeme tyto výroky hned, jakmile se budeme zabývat multiplikativním chováním nulového prvku o v okruhu.

Stejně jako v číselných oborech platí v každém okruhu $(R, +, .)$ rovnost $a.o = o$ pro každý prvek a okruhu. Snadno je totiž vidět, že $a.o = o$ vyplývá ze vztahů $a.o = a.o + o$ a $a.o = a.(o + o) = a.o + a\ o$ a z jednoznačné řešitelnosti rovnice $a.o = a.o + x$. Kromě toho je hned vidět, že i v každém tělese je součin roven nule, jakmile je alespoň jeden z činitelů nulový prvek. V okruhu $(\mathbf{Z}/(4), +, .)$ platí $(2)_4.(2)_4 = (0)_4$, tj. součin je kupodivu roven nulovému prvku, i když ten se mezi činiteli nevyskytuje. Věta, že součin je roven nule, právě když aspoň jeden z činitelů je nula, tedy v libovolném okruhu neplatí.

V tělese $(K, +, .)$ takové „pochybné" chování nemůže nastat, protože z předpokladu, že existují prvky tělesa $a \neq o$ a $b \neq o$, pro něž $a.b = o$, bychom vynásobením rovnosti prvkem a^{-1} dostali

$$a^{-1}.(a.b) = (a^{-1}.a).b = e.b = b = o,$$

a to odporuje předpokladu.

Existují okruhy s jednotkovým prvkem, v nichž je splněn požadavek, aby z $a.b = o$ vždy plynulo $a = o$ nebo $b = o$, pro všechny prvky okruhu. Jedním z těchto okruhů je např. okruh celých čísel, ve kterém používáme známým způsobem pojmy jako dělitel a prvočíslo a v němž platí věta o jednoznačném rozkladu každého prvku okruhu na součin mocnin prvočísel. Je zajímavé, že má smysl přenést uvedené pojmy na prvky libovolného okruhu, který splňuje předchozí podmínku, a že v každém takovém okruhu platí jednoduché výroky o relaci dělitelnosti (např. že z $a \mid b$ a $a \mid c$ plyne $a \mid (b + c)$, nebo že největší společný dělitel a nejmenší společný násobek prvků okruhu jsou vždy určeny jednoznačně). Ovšem největší společný dělitel dvou prvků nemusí v takových okruzích ještě existovat; jeho existence bude zaručena teprve dalšími dodatečnými pod-

mínkami. Totéž platí o obou shora uvedených větách o existenci a jednoznačnosti rozkladu na prvočinitele, na jejichž platnost se často díváme jako na samozřejmost. Že se nám použití pomocných prostředků teorie struktur hodí a že je často nutné, abychom byli s to řešit závažné matematické problémy, to ukazuje klasický problém řešitelnosti algebraických rovnic pomocí radikálů, který pochopí každý školák, jenž zná vzorečky pro řešení kvadratické rovnice:

Pro jaký stupeň n libovolné algebraické rovnice

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

jejíž koeficienty a_i jsou z tělesa reálných čísel, existuje vzorec na určení jejích kořenů? Už více než 300 let jsou takové vzorce známy pro rovnice 2., 3. a 4. stupně. Ale teprve využitím souhry pomocných prostředků z teorie grup a z teorie těles se Évaristu Galoisovi[11]) podařilo dokázat, že není možno udat vzorec pro řešení obecné rovnice více než čtvrtého stupně.

[11]) Évariste Galois (1811—1832) francouzský matematik; zakladatel moderního grupově teoretického zkoumání algebraických rovnic (Galoisovy teorie); mimo jiné zavedl pojem grupy a (algebraického) tělesa. Ty nejpodstatnější ze svých pronikavých matematických myšlenek uložil Galois v předvečer své smrti (byl zabit v souboji) v nejstručnější formě do dopisu, který považoval za svoji vědeckou závěť.

RŮZNÉ ČEPICE, A PŘESTO RODNÍ BRATŘI

4.3 ZOBRAZENÍ ZACHOVÁVAJÍCÍ STRUKTURU

Izomorfismy a homomorfismy

Ve studijní skupině sestavují studenti tabulky různých konečných grup, např.:

— grupy G_1 s prvky $f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = -x$, $f_4(x) = -\frac{1}{x}$ a se skládáním funkcí jakožto operací;

— G_2, aditivní grupy zbytkových tříd modulo 4; tedy $G_2 = \mathbb{Z}/(4)$;

— grupy G_3 s prvky 1, —1, i, —i a s operací násobení komplexních čísel (je potřeba jen vědět, že $i^2 = -1$);

— grupy G_4 s prvky

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{A}_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{A}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\mathbf{A}_4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

a s operací násobení matic.

Zvídavý čtenář by si měl před dalším čtením připravit tabulky těchto grup a ještě některých dalších, např. grupy nesoudělných zbytkových tříd modulo 12 (srov. tabulku v odstavci 4.1) a grupy otáčení čtverce kolem jeho středu s úhly $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ a s operací skládání.

Werner, nejmazanější z účastníků, náhle vysloví zprvu zarážející tvrzení, že G_1 a G_4 jsou „tytéž" grupy. Odůvodňuje to takto: „Když se podíváme na tabulky operací obou grup,

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

	$\mathbf{A}_1$	$\mathbf{A}_2$	$\mathbf{A}_3$	$\mathbf{A}_4$
$\mathbf{A}_1$	$\mathbf{A}_1$	$\mathbf{A}_2$	$\mathbf{A}_3$	$\mathbf{A}_4$
$\mathbf{A}_2$	$\mathbf{A}_2$	$\mathbf{A}_1$	$\mathbf{A}_4$	$\mathbf{A}_3$
$\mathbf{A}_3$	$\mathbf{A}_3$	$\mathbf{A}_4$	$\mathbf{A}_1$	$\mathbf{A}_2$
$\mathbf{A}_4$	$\mathbf{A}_4$	$\mathbf{A}_3$	$\mathbf{A}_2$	$\mathbf{A}_1$

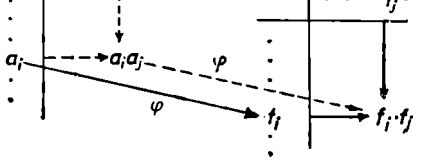
zjistíme, že se v nich počítá úplně stejně. Dokonce bychom mohli sestavit abstraktní počtní tabulku a podle toho, zda budeme prvky a_1, a_2, a_3, a_4 interpretovat jako čtyři funkce f_1, ..., f_4, nebo jako čtyři matice $\mathbf{A}_1$, ..., $\mathbf{A}_4$ (a odpovídajícím způsobem operaci . jednou jako skládání funkcí, podruhé jako násobení matic), dostaneme tabulku ‚konkrétní' grupy G_1, resp. G_4. Grupy G_1 a G_4 jsou tedy ‚v podstatě' stejné, odlišují se jaksi jen ve své konkrétní podobě, ve způsobu popisu. Jsou to tedy rodní bratři, nosí jen odlišné čepice."

.	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_1	a_4	a_3
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_3	a_2	a_1

To ostatním otvírá oči, přesto se Kristýna odvažuje namítnout, že tabulka operace G_1 bude přeci vypadat docela jinak, když prvky G_1 jinak očíslujeme, aniž by se přitom v grupě samé něco změnilo. Všichni se rychle shodují na tom, že „strukturně totožné" grupy by měly být takové, jejichž tabulky operací se při vhodném přečíslování prvků liší nejvýše označením. „Ale pak jsou přece totožné i G_2 a G_3," objevuje Grit, „stačí přece jenom navzájem přiřadit prvky $(0)_4$ a 1, $(1)_4$ a i, $(2)_4$ a —1 a $(3)_4$ a —i, a dostaneme shodné tabulky." Přesvědčte se, zda má Grit pravdu! „Možná, že tato strukturní totožnost není nic vzrušujícího," uvažuje Uwe, starý skeptik, „možná, že jsou grupy se stejným počtem

prvků, třeba 4, vždy totožné.“ Ale Werner to po chvíli přemýšlení může vyvrátit: „Spojíme-li v grupách G_1 a G_4 některý prvek sám se sebou, dostaneme vždy neutrální prvek, v grupách G_2 a G_3 se to ale stane jen ve dvou případech ze čtyř. Nemohou tedy být např. G_1 a G_2 strukturně totožné.“ Na tomto místě zasáhne vedoucí kroužku poznámkou, že Grit předtím odhalila metodu, s níž je možné pojem strukturní totožnosti — v matematice nazývané *izomorfie* (řecky: stejný tvar) — přenést na nekonečné grupy. Místo o „vhodném přečíslování“ prvků pak obecněji mluvíme o „vzájemně jednoznačném přiřazení“ φ mezi prvky jedné a druhé grupy. Výrok o „strukturní totožnosti“ pak dostane tvar: Jsou-li prvkům a, b jedné grupy přiřazeny prvky $\varphi(a)$, $\varphi(b)$ druhé grupy, musí být vzájemně přiřazeny i součiny $a.b$ a $\varphi(a).\varphi(b)$, tj. musí platit $\varphi(a.b) = \varphi(a).\varphi(b)$. V této rovnosti je třeba si uvědomit, že znak „.“ nalevo označuje operaci v jedné grupě a napravo operaci v druhé grupě.

Zobrazení φ s touto vlastností se nazývá zachovávající operaci (resp. relaci, neboť každou operaci můžeme chápat jako relaci). U konečných grup se vlastnost vzájemně jednoznačného zobrazení zachovávat operaci



Obr. 29
plná čára: nejprve zobrazeno, potom složeno $\varphi(a_i).\varphi(a_j) = f_i.f_j$
čárkovaně: nejprve složeno, potom zobrazeno $\varphi(a_i.a_j) = f_i.f_j$

projeví ve shodné stavbě tabulky operace; tuto situaci ilustruje obr. 29.

Definice 4.6. Grupa $(G_1, \circ_1)$ se nazývá *izomorfní* s grupou $(G_2, \circ_2)$, právě když zároveň platí:
(1) Existuje vzájemně jednoznačné zobrazení φ grupy G_1 na G_2;
(2) φ zachovává operaci, tj. pro všechna $a, b \in G_1$ platí

$$\varphi(a \circ_1 b) = \varphi(a) \circ_2 \varphi(b).$$

Zobrazení φ se nazývá *izomorfismus* G_1 *a* G_2.

Nyní lze snadno zjistit, že grupa $(\mathbf{R}^+, .)$ kladných reálných čísel vzhledem k násobení je izomorfní aditivní grupě $(\mathbf{R}, +)$ reálných čísel, neboť dobře známe zobrazení $\varphi(x) = \log x$ mezi $\mathbf{R}^+$ a $\mathbf{R}$, které díky

$$\varphi(xy) = \log xy = \log x + \log y = \varphi(x) + \varphi(y)$$

zachovává operaci. Na základě této izomorfie mezi $(\mathbf{R}^+, .)$ a $(\mathbf{R}, +)$ spočívá, jak známo, počítání s logaritmy a logaritmickým pravítkem: délka úseku příslušná součinu se dostane jako součet délek příslušných jednotlivých činitelům.

Relace „je izomorfní s" mezi grupami je relací ekvivalence (srov. odstavec 2.3), o čemž se snadno přesvědčíme; nazývá se *izomorfie*. V třídách ekvivalence se pak sejdou právě všechny navzájem strukturně totožné grupy. Kdybychom mohli získat přehled o všech třídách ekvivalence (k tomu by stačilo znát z každé třídy jednoho reprezentanta), ovládali bychom dokonale každou konkrétní grupu a hlavní úloha teorie grup by tak byla splněna. Tento problém není dodnes vyřešen*); musíme

*) Problém klasifikace prostých konečných grup (tj. jakýchsi stavebních kamenů, z nichž lze „složit" každou grupu) byl vyřešen počátkem 80. let. Úplný důkaz zabírá přibližně 15 000 stránek odborných časopisů. Zájemce odkazujeme na populární článek D. Gorensteina v čas. Scientific American, December 1985 (ruský překlad В мире науки, No 2, 1986).

se proto spokojit s tím, že se seznámíme s co největším množstvím strukturních typů. Plně např. ovládáme cyklické grupy; v odstavci 4.2 jsme viděli, že každá cyklická grupa s n prvky je izomorfní aditivní grupě zbytkových tříd modulo n a každá nekonečná cyklická grupa je izomorfní aditivní grupě celých čísel. Odpovídající vzájemně jednoznačná zobrazení zachovávající operaci jsou $\varphi(a^m) = (m)_n$, resp. $\varphi(a^m) = m$.

Analogicky můžeme zavést pojem izomorfie i pro jiné struktury, např. pro okruhy. Protože to jsou struktury se dvěma operacemi, je vlastnost zachování operace vyjádřena dvěma rovnostmi:

$$\varphi(a \oplus b) = \varphi(a) + \varphi(b) \text{ a } \varphi(a \odot b) = \varphi(a).\varphi(b).$$

Vlastnost φ zachovávat operaci slouží dokonce i k tomu, že se strukturní vlastnosti vzoru při zobrazení φ přenesou na obraz Platí např.:

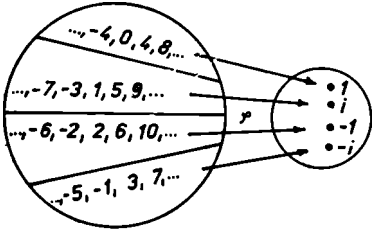
$$\left.\begin{array}{l}(G_1, \circ_1) \text{ grupa;}\\ (G_2, \circ_2) \text{ množina s operací;}\\ (G_1, \circ_1) \text{ izomorfní s } (G_2, \circ_2)\end{array}\right\} \Rightarrow (G_2, \circ_2) \text{ rovněž grupa.}$$

K tomuto závěru jsme však vůbec nepoužili vzájemnou jednoznačnost; už prostá zobrazení zachovávající operaci zachovávají strukturu grupy. Má proto smysl studovat i taková zobrazení. Takové např. bude zobrazení φ mezi aditivní grupou $\mathbf{Z}$ celých čísel a grupou G_3, položíme-li

$$\varphi(n) = \begin{cases} 1, \text{ jestliže } n \equiv 0 \pmod 4,\\ \mathrm{i}, \text{ jestliže } n \equiv 1 \pmod 4,\\ -1, \text{ jestliže } n \equiv 2 \pmod 4,\\ -\mathrm{i}, \text{ jestliže } n \equiv 3 \pmod 4.\end{cases}$$

Takovéto zobrazení se nazývá *homomorfismus* a grupa $\mathbf{Z}$ se nazývá *homomorfní s grupou* G_3. Přesvědčte se, že

homomorfismus φ znázorněný na obr. 30 zachovává operaci! (Návod: nejprve uvažte, že φ můžete psát ve tvaru $\varphi(n) = \mathrm{i}^n$ pro všechna $n \in \mathbf{Z}$).



Obr. 30

Zformulujme definici pojmu „homomorfismus" tentokrát pro okruhy:

Definice 4.7. Okruh $(R_1, +_1, \circ_1)$ se nazývá *homomorfní* s okruhem $(R_2, +_2, \circ_2)$, právě když zároveň platí:
(1) existuje prosté zobrazení φ okruhu R_1 na R_2;
(2) φ zachovává operaci, tj. pro všechna $a, b \in R_1$ platí

$$\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b)$$

a

$$\varphi(a \circ_1 b) = \varphi(a) \circ_2 \varphi(b).$$

Z definic D(4.6) a D(4.7) plyne, že každý izomorfismus je také homomorfismus. Obrácený výrok však neplatí.

Vraťme se k předchozímu příkladu grup $\mathbf{Z}$ a G_3. Protože zobrazení φ je (jen) prosté, bylo by nasnadě rozdělit definiční obor φ, tedy $\mathbf{Z}$, na třídy prvků se stejným obrazem. Snadno nahlédneme, že tyto třídy jsou právě zbytkové třídy modulo 4, které samy tvoří grupu G_2 vzhledem ke sčítání.

Je-li obecně φ homomorfní zobrazení G na G', víme z odstavce 1.7, že rozdělení definičního oboru G zobrazením φ na třídy prvků se stejným obrazem je rozklad, a dále z 2.3 je nám známo, že tento rozklad můžeme dostat jednoznačně určenou relací ekvivalence R. V našem příkladu to zřejmě je kongruence modulo 4; srov. obr. 30. To, že φ zachovává operaci, má ten důsledek, že tato relace ekvivalence je dokonce kongruencí (srov. odstavec 3.4); Z aRa' a bRb' plyne $(a.b)R(a'.b')$, neboť aRa' (resp. bRb') znamená, že $\varphi(a) = \varphi(a')$ (resp. $\varphi(b) = \varphi(b')$), a díky tomu, že φ zachovává operaci, je $\varphi(a.b) = \varphi(a).\varphi(b) = \varphi(a').\varphi(b') = \varphi(a'.b')$, tedy $(a.b)R(a'.b')$. Můžeme proto v podílové množině G/R zavést operaci pomocí reprezentantů (srov. odstavec 3.4); v našem příkladu je to sčítání zbytkových tříd modulo 4. Takto vzniklá aditivní grupa zbytkových tříd modulo 4 je pak — jak už víme —, dokonce izomorfní grupě G_3. To nám dává příležitost k položení otázky: „Vyplývá z homomorfie G a G' vždy izomorfie G/R a G', je-li G/R rozklad G na třídy prvků se stejnými obrazy při φ (φ je homomorfismus G na G')?“ Na tuto otázku můžeme odpovědět kladně: *Je-li φ prosté zobrazení G na G' zachovávající operaci a označuje-li $[a]$ třídu všech prvků G se stejným obrazem $\varphi(a)$, je zobrazení ψ, kde $\psi([a]) = \varphi(a)$, vzájemně jednoznačné zobrazení G/R na G', které zachovává operaci.*

Dalším důsledkem pro homomorfismus φ zachovávající operaci je, že shora uvedená relace R je už jednoznačně určena třídou U všech prvků G, jejichž obrazem je neutrální prvek e' grupy G', neboť platí: $aRb \Leftrightarrow$ $\Leftrightarrow a.b^{-1} \in U$. Tato množina U se nazývá *jádro* homomorfismu φ. Důkaz dostaneme snadno výpočtem:

$$aRb \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow \varphi(a).\varphi(b)^{-1} = e' \Leftrightarrow$$
$$\Leftrightarrow \varphi(a).\varphi(b^{-1}) = \varphi(a.b^{-1}) = e' \Leftrightarrow a.b^{-1} \in U.$$

V našem příkladu je U množina všech celočíselných násobků čtyř, neboť dva prvky $a, b \in \mathbf{Z}$ mají týž obraz při φ, právě když $a \equiv b \pmod 4$, tj. když $a - b \equiv 0 \pmod 4$, čili $a - b \in U$. Protože grupová operace v našem příkladu je sčítání, nemůže se nikdo divit, že jsme místo $a.b^{-1}$ psali $a + (-b) = a - b$.

Právě provedená úvaha, že homomorfní zobrazení φ G na G' je už jednoznačně určeno svým jádrem, dává podnět k otázce: „Jaké vlastnosti jsou nutné a stačí, aby neprázdná podmnožina $U \subset G$ byla jádrem homomorfismu?" Kdybychom totiž mohli udat všechny podmnožiny $U \subset G$, které mohou být jádrem homomorfního zobrazení G, měli bychom přehled o všech homomorfních obrazech G. Této otázce se budeme ještě věnovat v příštím odstavci.

ROSTOUCÍ ZÁSOBY

4.4 ODVOZENÉ STRUKTURY

Jak můžeme získat další struktury

Už v 1. kapitole jsme viděli, jak se dají vytvářet další množiny, začneme-li jednou množinou M. Můžeme kupříkladu uvažovat podmnožiny M nebo přejít ke kartézskému součinu $M \times M$, anebo pomocí relace ekvivalence R utvořit podílovou množinu M/R. Pokusme se tímto způsobem zvětšit také naši zásobu struktur, např. grup.

a) Podstruktury

Je-li $(G, .)$ grupa a U neprázdná podmnožina G, $(U, .)$ není obecně grupa. Kupříkladu množina prvočísel P je sice podmnožinou $\mathbf{Z}$, ale $(P, +)$ není grupa, protože je např. $3 \in P$, $5 \in P$ a $3 + 5 = 8$, ale $8 \notin P$.

Nemůžeme tedy chápat $(P, +)$ jako podgrupu $(\mathbf{Z}, +)$. Naproti tomu splňuje-li podmnožina $U \subset G$ sama axiómy grupy vzhledem k operaci definované v grupě G[12]), nazýváme $(U, .)$ *podgrupou* $(G, .)$. Tak kladná racionální čísla tvoří vzhledem k násobení podgrupu grupy $(\mathbf{R} \setminus \{0\}, .)$. Všechny axiómy grupy jsou už splněny, jakmile je U uzavřená vůči dané operaci a přitom inverzní prvek ke každému prvku z U patří opět do U. Neboť je-li splněn asociativní zákon pro všechny prvky z G, platí tím spíš i pro všechny prvky z U. Neutrální prvek e, který je k dispozici v G, patří za uvedeného předpokladu určitě i do U, neboť je-li $U \neq \emptyset$, existuje $a \in U$, a tudíž také $a.a^{-1} = e \in U$. Můžeme proto říci: Je-li $(G, .)$ grupa, U neprázdná podmnožina G, je $(U, .)$ podgrupa $(G, .)$, právě když pro $a \in U$ a $b \in U$ vždy také platí $a.b \in U$ a $a^{-1} \in U$.

Příklady. Každá grupa $(G, .)$ obsahuje dvě triviální podgrupy, totiž samotnou G a podgrupu, jež sestává jen z neutrálního prvku e. V aditivní grupě celých čísel tvoří všechny násobky pevného celého čísla m podgrupu. Naproti tomu např. množina lichých čísel není podgrupa $(\mathbf{Z}, +)$, neboť součet dvou lichých čísel je sudý. Grupa G_3 z odstavce 4.3 s prvky 1, —1, i a —i obsahuje podgrupu s prvky 1 a —1.
V grupě všech permutací 4 prvků (srov. odstavec 3.1) množina

$$V = \left\{\pi_0 = \begin{pmatrix}1234\\1234\end{pmatrix}, \pi_1 = \begin{pmatrix}1234\\2143\end{pmatrix}, \pi_2 = \begin{pmatrix}1234\\3412\end{pmatrix}, \pi_3 = \begin{pmatrix}1234\\4321\end{pmatrix}\right\}$$

tvoří podgrupu vzhledem ke skládání, o čemž se nejlépe přesvědčíte utvořením tabulky operace ve V.

[12]) Přesněji neuvažujeme v U tutéž operaci jako v G, nýbrž zúžení dané operace na U.

Analogickým způsobem můžeme také zavést podokruhy a podtělesa; jistě vám nebude zatěžko na základě pojmu „podgrupy" objasnit, co se rozumí „podokruhem". Kupříkladu množina všech diagonálních matic — to jsou $n \times n$ matice s vlastností $a_{ik} = 0$ pro $i \neq k$ —, tvoří vzhledem ke sčítání a násobení matic okruh, a je tedy rovněž podokruhem okruhu všech $n \times n$ matic. Jako nejjednodušší příklad budiž zmíněn podokruh sudých čísel v okruhu celých čísel. Těleso reálných čísel obsahuje jako podtěleso těleso racionálních čísel.

Nyní se můžeme vrátit k otázce položené na konci odstavce 4.3, které podmnožiny U grupy G mohou být jádrem homomorfismu φ grupy G. Jádro U homomorfismu φ je, jak už víme, množina všech prvků $a \in G$, pro něž $\varphi(a) = e'$. Přitom G označuje grupu vzorů, G' grupu obrazů, e (resp. e') neutrální prvek G (resp. G'). Určitě je $e \in U$, tj. $\varphi(e) = e'$, jak okamžitě dostaneme z rovností $\varphi(a).e' = \varphi(a) = \varphi(a.e) = \varphi(a).\varphi(e)$ díky vlastnosti krácení grupové operace. Je-li $a, b \in U$, tedy $\varphi(a) = \varphi(b) = e'$, pak také platí $\varphi(a.b) = \varphi(a).\varphi(b) = e'.e' = e'$, to ale dává $a.b \in U$. Dále je pro $a \in U$ také $a^{-1} \in U$, neboť máme

$$\varphi(a^{-1}) = \varphi(a^{-1}).e' = \varphi(a^{-1}).\varphi(a) = \varphi(a^{-1}.a) = \varphi(e) = e'.$$

Jako „vedlejší produkt" můžeme z těchto rovností také dostat vztah $\varphi(a^{-1}).\varphi(a) = e'$, a tedy $\varphi(a^{-1}) = \varphi(a)^{-1}$; jinými slovy: obraz prvku inverzního k a se rovná inverznímu prvku k obrazu a. Tohoto poznatku jsme už mlčky využili v odstavci 4.3. Vyhledejte si sami příslušné místo!

Naše úvahy ukázaly toto: K tomu, aby neprázdná podmnožina U grupy G mohla být jádrem homomorfismu grupy G, je nutné, aby byla podgrupou.

Dá se ukázat, že pro komutativní grupy je tato pod-

mínka také postačující; pro nekomutativní grupy naproti tomu nemůže být každá podgrupa jádrem homomorfismu, musíme se omezit na jisté podgrupy splňující další podmínku a nazývané také normální podgrupy. Analogické výroky platí pro okruhy; jádro každého okruhového homomorfismu, tj. množina všech prvků okruhu vzorů, jejichž obraz je nulový prvek okruhu obrazů, musí být podokruh. Obrácené tvrzení platí jen pro komutativní okruhy, jinak se musíme uchýlit k speciálním podokruhům, tzv. ideálům. Hlubší rozbor by už překračoval rámec této knížky.

b) Součinové struktury

Další možnost, jak získat ze známých struktur nové, spočívá v přechodu ke kartézským součinům. Jsou-li např. $(G_1, \circ_1)$ a $(G_2, \circ_2)$ grupy, stane se kartézský součin $G = G_1 \times G_2$ grupou, definujeme-li v G operaci $\circ$ takto:

$$(a_1, a_2) \circ (b_1, b_2) = (a_1 \circ_1 b_1, a_2 \circ_2 b_2),$$

tj. násobíme-li v G po složkách. Zřejmě je G uzavřená vzhledem k $\circ$, neutrální prvek je (e_1, e_2) a prvek (a_1^{-1}, a_2^{-1}) je inverzní k (a_1, a_2). Konečně jednoduchý výpočet, který můžete provést sami, ukáže, že operace $\circ$ je také asociativní. $(G, \circ)$ se nazývá *direktní součin grup* $(G_1, \circ_1)$ a $(G_2, \circ_2)$. Stejně můžeme postupovat i u jiných struktur, např. u okruhů. Není přitom nutné zavádět operaci v kartézském součinu po složkách; i jiné definice součtu a součinu mohou vést opět ke struktuře okruhu (což se ale vždy musí napřed prozkoumat). Přejdeme-li příkladně od tělesa $\mathbf{R}$ reálných čísel ke kartézskému součinu $\mathbf{R} \times \mathbf{R}$ s operacemi

$$(a_1, a_2) \oplus (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$
$$(a_1, a_2) \odot (b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1),$$

je také $(\mathbf{R} \times \mathbf{R}, \oplus, \odot)$ těleso, jež je izomorfní s tělesem

komplexních čísel. To je hned vidět, píšeme-li místo (a_1, a_2) obvyklé $a_1 + ia_2$; pak je předchozími definicemi sčítání a násobení charakterizováno obvyklé sčítání a násobení komplexních čísel.

c) Podílové struktury

Vyjdeme-li z algebraické struktury, např. grupy $(G, .)$, můžeme také další takové struktury získat uvažováním homomorfních obrazů dané struktury. Z odstavce 4.3 víme, že to je totéž jako přejít k podílové množině G/R podle relace kongruence R a definovat operaci mezi třídami ekvivalence pomocí reprezentantů. Tímto způsobem dostaneme tzv. *podílovou strukturu*, jež bude stejného typu jako výchozí struktura. Je-li tedy $(G, .)$ grupa, je $(G/R, \circ)$ také grupa, nazývaná *podílová grupa* nebo *faktorová grupa* G podle R. Touto konstrukční metodou vznikne např. z aditivní grupy $(\mathbf{Z}, +)$ celých čísel aditivní grupa zbytkových tříd modulo m, vezmeme-li jako relaci kongruence R obvyklou kongruenci celých čísel modulo m, resp. z okruhu $(\mathbf{Z}, +, .)$ celých čísel vznikne okruh zbytkových tříd modulo m.

d) Jako velmi plodná se ukazuje kombinace různých možností pro vytváření nových struktur; občas tak dokonce vzniknou „vyšší struktury". Předvedeme to na přechodu od okruhu $(\mathbf{Z}, +, .)$ celých čísel k tělesu $(\mathbf{Q}, +, .)$ racionálních čísel. Z algebraického hlediska získáme $(\mathbf{Q}, +, .)$ jako podílovou strukturu kartézského součinu $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$. Přejdeme totiž nejprve od $\mathbf{Z}$ k množině $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ všech uspořádaných dvojic (a, b) celých čísel, jež obvykle píšeme ve tvaru a/b a nazýváme zlomky (druhá složka je $b \neq 0$; proto $\mathbf{Z} \setminus \setminus \{0\}$). Podílová rovnost $=_Q$ definovaná vztahem

$$\frac{a}{b} =_Q \frac{c}{d}, \text{ právě když } ad = cb,$$

je relace ekvivalence R, a v podílové množině $(\mathsf{Z} \times (\mathsf{Z} \setminus \{0\}))/R$ můžeme tedy definovat sčítání a násobení pomocí reprezentantů vztahy

$$\left[\frac{a}{b}\right] \oplus \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right]; \quad \left[\frac{a}{b}\right] \odot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right],$$

protože podílová rovnost mezi zlomky se ukazuje jako snášenlivá k operacím $+$ a $.$, tj. jako relace kongruence. Třídy se nazývají racionální čísla. Postup, objasněný zde na příkladu, kterým lze přejít od okruhu k tělesu tak, že uvažujeme „podíly" $\frac{a}{b}$ obecně v okruhu nedefinované a mezi nimi zavedeme operace zcela analogicky k počítání se zlomky, se nechá dále zobecnit. Je-li R komutativní okruh s jednotkovým prvkem e, v němž se součin rovná nule právě tehdy, je-li alespoň jeden z činitelů nula, přesněji nulový prvek, dojdeme vždy popsaným způsobem — vycházejíce z R —, k tělesu K. To se nazývá *podílové těleso okruhu* R a má následující vlastnosti:

— V K existuje podokruh $\bar{R}$ izomorfní s R (v našem příkladu množina všech racionálních čísel $\left[\frac{a}{1}\right]$), čemuž pak můžeme stručně říkat, že „K obsahuje R".

— Mezi všemi tělesy, která obsahují R, je K nejmenší (pro náš příklad to znamená, že neexistuje těleso, jež by leželo mezi okruhem celých čísel a tělesem racionálních čísel).

— K je až na izomorfismus jednoznačně určeno, a speciálně tudíž nezávisí na způsobu konstrukce (proto také dostaneme těleso racionálních čísel, i když přejdeme nejprve od polookruhu přirozených čísel k polotělesu nezáporných zlomků a od těch pak přidáním odpovídajících „záporných" čísel k tělesu čísel racionálních).

4.5 CVIČENÍ

1. Doplňte tabulku v odstavci 4.1 a odůvodněte zápisy.

2. Zjistěte, zda následující objekty mají vlastnost pologrupy, grupy či komutativní grupy:

a) $(\mathscr{P}(M), \bigcap)$, b) $(M_{(2;2)}, .)$,
c) $(\mathbf{Q}^*, .)$, d) $(\mathbf{R}, .)$,
e) $(U, \circ)$, kde $U = \{1, 2, 3, \ldots, 12\}$
a

$$a \circ b = \begin{cases} a + b, & \text{jestliže } a + b \leqq 12, \\ a + b - 12, & \text{jestliže } a + b > 12 \end{cases}$$

(operaci $\circ$ bychom mohli nazvat „hodinové sčítání“);
f) množina S všech spojitých funkcí definovaných na uzavřeném intervalu $\langle a, b\rangle$ s operací sčítání funkcí;
g) množina L všech lineárních funkcí definovaných na uzavřeném intervalu $\langle a, b\rangle$ s operací sčítání funkcí;
h) množina všech matic tvaru (1) pro $0 \leqq \varphi < 2\pi$ s násobením matic.

$$(1) \quad \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

3. a) Je tabulka 1 tabulkou grupy?
b) Doplňte tabulku 2 tak, aby to byla tabulka grupy.
c) Jaký prvek musí stát v tabulce 3 na místě otazníku, je-li to tabulka grupy?

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

	a_1	a_2	a_3	a_4	a_5
a_1				a_4	
a_2			a_3	a_4	
a_3					
a_4					
a_5					

	.		.	
	⋮		⋮	
.	…	e	…	a …
	⋮		⋮	
.	…	b	…	? …
	⋮		⋮	

4. Zjistěte, zda následující objekty mají vlastnosti okruhu či tělesa:

a) $(M_{(2;2)}, +, .)$, b) $(\mathbf{Q}^*, +, .)$,

c) $(\mathbf{Z}/(4), +, .)$, d) $(\mathbf{Z}/(3), +, .)$,

e) množina všech uspořádaných dvojic (a, b) reálných čísel se sčítáním a násobením definovaným po složkách;

f) množina z cvičení e), přičemž teď je násobení definováno vztahem

$(a_1, b_1).(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$.

5. Dokažte:

a) Každá konečná regulární pologrupa je grupa.

b) Neutrální prvek grupy $(G, \circ)$ je zároveň neutrálním prvkem každé její podgrupy $(U, \circ)$,

c) Sjednocení dvou podgrup téže grupy není nutně zas podgrupa nějaké grupy.

d) V okruhu pro libovolné prvky a, b platí pravidla: $(-a)b = -(ab)$, $a(-b) = -(ab)$, $(-a)(-b) = ab$.

e) V každém tělese platí binomická věta, např. $(a + b)^2 = a^2 + 2ab + b^2$.

6. Zkonstruujte těleso se dvěma (resp. se třemi) prvky prostřednictvím tabulky.

7. Prověřte, zda následující zobrazení jsou izomorfismy či homomorfismy (n značí pevně zvolené přirozené číslo a $\mathbf{R}^+$ jsou kladná reálná čísla):

a) φ zobrazuje $(\mathbf{R}, +)$ na $(\mathbf{R}, \div)$, kde $\varphi(a) = na$ pro všechna $a \in \mathbf{R}$;

b) φ zobrazuje $(\mathbf{R}^+, .)$ na $(\mathbf{R}^+, .)$, kde $\varphi(a) = a^n$ pro všechna $a \in \mathbf{R}^+$;

c) φ zobrazuje $(\mathbf{R} \setminus \{0\}, .)$ na $(\mathbf{R}^+, .)$, kde $\varphi(a) = |a|$ pro všechna $a \in \mathbf{R} \setminus \{0\}$;

d) φ zobrazuje $(\mathscr{P}(M), \cap)$ na $(\mathscr{P}(M), \cup)$, kde $\varphi(A) = A'$ pro všechna $A \in \mathscr{P}(M)$;

e) φ zobrazuje $(\mathbf{C}, .)$ na $(\mathbf{C}, .)$, kdo $\varphi(z) = \bar{z}$ pro všechna $z \in \mathbf{C}$ ($\bar{z}$ je komplexně sdružené číslo k z).

8. a) Ukažte, že grupa G_1 z odstavce 4.3 je izomorfní s grupou nesoudělných zbytkových tříd modulo 8.
   b) Definujte homomorfní zobrazení φ grupy $(Z, +)$ na $(H, +)$, kde $(H, +)$ je nějaká dvouprvková grupa.
   c) Ukažte: Aditivní grupa zbytkových tříd modulo 6 a multiplikativní grupy nesoudělných zbytkových tříd modulo 7 a 9 jsou navzájem izomorfní. Aditivní grupa zbytkových tříd modulo 6 je cyklická; co z toho vyplývá pro obě další grupy?
   d) Zjistěte, pro které grupy $(G, \circ)$ je zobrazení φ, kde $\varphi(a) = a^{-1}$ pro všechna $a \in G$, izomorfismus $(G, \circ)$ na sebe.

9. a) Zjistěte všechny vlastní podgrupy multiplikativní grupy nesoudělných zbytkových tříd modulo 15.
   b) Určete všechny podgrupy cyklické grupy řádu 12 a pro každou udejte vytvořující prvek.
   c) Udejte všechny homomorfní obrazy multiplikativní grupy nesoudělných zbytkových tříd modulo 15. (Návod: použijte řešení úlohy 9a; tím jsou nalezena jádra všech homomorfismů.)