Algebra, každý začátek je lehký

ŠKOLA MLADÝCH MATEMATIKŮ

ALGEBRA
KAŽDÝ ZAČÁTEK JE LEHKÝ

58

Vydal ÚV matematické olympiády v nakladatelství Mladá fronta

ŠKOLA MLADÝCH MATEMATIKŮ

HERBERT KÄSTNER, PETER GÖTHNER

ALGEBRA
Každý začátek je lehký

PŘELOŽIL KAREL HORÁK

PRAHA 1986
VYDAL ÚV MATEMATICKÉ OLYMPIÁDY
V NAKLADATELSTVÍ MLADÁ FRONTA

Recenzoval RNDr. Milan Koman, CSc.

PŘEDMLUVA

„Dítě, které se spálí, se má před ohněm na pozoru", a to před každým ohněm, ačkoli se spálilo jen o jeden určitý plamen; zobecnilo totiž svoji zkušenost. My zas chceme v této knížečce zobecnit mnohé z našich zkušeností s matematikou. Uvidíme například, že rozdělení racionálních čísel na třídy ekvivalentních zlomků podobně jako rozdělení trojúhelníků do tříd shodných trojúhelníků anebo rozdělení soustav lineárních rovnic do tříd navzájem ekvivalentních soustav spočívá na stejném myšlenkovém principu. Takové zajímavé analogie a překvapivé souvislosti mezi zdánlivě vzdálenými oblastmi nám umožní uspořádat a systemizovat jejich matematický obsah.

Podobných analogií si všimneme také při vyšetřování vlastností početních operací v daných množinách; např. stejným „početním pravidlům" podléhá jak násobení racionálních čísel, tak sčítání vektorů nebo skládání otočení kolem daného bodu v rovině či sčítání funkcí. Zřejmě není podstatné, s čím počítáme, ale jak počítáme, proto je výhodné odhlédnout od konkrétních vlastností prvků dané množiny a od významu dané operace a zkoumat obecnou množinu prvků s nějakou operací, která splňuje jistá, dobře definovaná pravidla. Takovýto přístup vede k pojmu algebraické struktury a každá množina s libovolnou konkrétní operací, která uvedená pravidla rovněž splňuje, je pak modelem dané struktury. Znamenalo by to však zůstat stát v půli

cesty, kdybychom se spokojili s tím, že další abstrakcí matematických poznatků získáme nové pojmy, s kterými budeme moci tyto poznatky uspořádat a systemizovat. Ono se ukazuje, že z poměrně malého počtu pravidel, tzv. axiómů, můžeme odvodit soustavu pravidel a vybudovat tak celou teorii dané struktury. Tyto obecné zákonitosti platí v každém konkrétním modelu struktury, takže je pak už nemusíme v každém jednotlivém případě znovu odvozovat — jejich důkaz byl proveden v teorii odpovídající struktury. To je velkou předností strukturálního uvažování, navíc získáme na jasnosti a přesnosti. Nadto nám takto získané algebraické znalosti umožní poměrně rychlý přístup k speciálním matematickým oblastem — jako „vedlejší produkt" se kromě jiného naučíme počítat s maticemi a se zbytkovými třídami celých čísel.

Cílem naší knihy je přivést čtenáře k strukturálnímu myšlení a povzbudit jeho chuť k dalšímu studiu algebraických struktur, přičemž bychom mu chtěli pro toto studium poskytnout solidní základy.

„Každý začátek (algebry) je lehký," slibuje název tohoto svazečku. To ovšem u každého, kdo se chce matematikou zabývat doopravdy, předpokládá spolupráci, samostatné řešení některých úloh a příležitostné opakování. I když tedy nemůžeme nabídnout pohodlnou cestu k algebře, vynasnažíme se ji pokud možno usnadnit tím,

— že začneme vždy elementárními otázkami a srozumitelnými příklady a k přesnému pochopení předmětu se dopracujeme postupně;
— že mnoha příkladů budeme používat opakovaně a v různých problémových situacích;
— že poměrně obsáhlým výkladem v počátečních kapitolách čtenáře dobře připravíme k zdolání překážek v závěru.

Abychom usnadnili zavedení algebraických struktur,

věnujeme samostatné kapitoly relacím a operacím, neboť již zde je obsaženo velmi mnoho „algebraického". V úvodní části věnované množinám může čtenář podle svých znalostí některé odstavce případně vynechat.

Matematické znaky a symboly, jejichž znalost nelze předpokládat, budou vysvětleny přímo na místě, jinak budeme používat obvyklého značení: $\mathbb{N}_0$ pro množinu všech celých nezáporných čísel, $\mathbb{Z}$ pro množinu všech celých čísel a pomocí $\mathbb{Q}^*$, $\mathbb{Q}$ a $\mathbb{R}$ označíme množinu zlomků (s celočíselným čitatelem a jmenovatelem), množinu všech racionálních čísel a množinu všech reálných čísel. Důležité definice a věty budou číslovány průběžně, takže např. „def. 3.4" označuje 4. definici 3. kapitoly a analogicky „věta 2.3" 3. větu 2. kapitoly. Zkráceně se na ně budeme v dalším textu odvolávat jako na D(3.4), V(2.3) apod.

Každá ze čtyř kapitol je zakončena množstvím úloh a cvičení, jejichž řešení jsou uvedena na konci knihy.

Ke studiu naší knížečky plně dostačuje učivo základní školy a je určena těm žákům, kteří mají zájem o matematiku, ale užitečná může být i studentům prvního semestru vysokých škol a samozřejmě též učitelům matematiky.

Lipsko červen 1983 *Autoři*

I. MNOŽINY

MNOŽINA TRAMPOT S MATEMATIKOU

1.1 POJEM MNOŽINY

Čtenář se dozví, jak se v matematice používá pojem „množina"

Představa, že s matematikou jsou nějaké trampoty, se nám nelíbí — doufáme naopak, že naše knížka přinese čtenáři množinu příjemných chvil a on sám učiní množství zajímavých objevů.

Nikdo z nás teď zřejmě nemá jasnou představu o tom, co se míní množinou příjemných chvil či množinou trampot, stejně jako nevíme, co to je množství[1]) peněz.

Než přikročíme k přesnějšímu objasnění pojmu množiny, uveďme raději ještě několik příkladů:

M_1: množina čísel 1, 2, 3, 7;

M_2: množina všech prvočísel;

M_3: množina všech racionálních čísel, která jsou řešením rovnice $5x + 3 = -0{,}5$;

M_4: množina všech reálných čísel, která jsou řešením rovnice $x^2 + 9 = 0$;

M_5: množina všech tříd základní školy ve Štěpánské ulici v Praze;

M_6: množina, která obsahuje pouze slovo „množina";

M_7: množina všech dělitelů čísla 24;

M_8: množina všech přímek v rovině, které jsou navzájem kolmé.

---

[1]) Připomeňme zde, že pojem množiny zavedl do matematiky německý matematik Georg Cantor (1845—1918). Ten k označení nového pojmu zvolil německé slovo „Menge", které má význam „množství", v češtině se však toto slovo neujalo, a bylo později nahrazeno novým slovem „množina". (Pozn. překl.)

Na rozdíl od předchozích slovních spojení, ve kterých jsme použili slova „množina" místo obvyklého slova „množství", můžeme v příkladech M_1 až M_8 rozhodnout, zda nějaký objekt našeho hmotného či myšlenkového světa v dané množině leží či nikoliv. Objektům ležícím v nějaké množině budeme říkat prvky množiny.

Naše příklady objasňují, jakými způsoby můžeme množinu popsat. V některých případech toho dosáhneme přímým výčtem všech prvků množiny: $M_1 = \{1, 2, 3, 7\}$, $M_3 = \{-0{,}7\}$, $M_6 = \{\text{množina}\}$. Při výčtu prvků množiny M_5 nesmíme přehlédnout, že jejími prvky nejsou žáci, nýbrž třídy, tj. množiny žáků. Popis množiny výčtem jejích prvků by však selhal u takových množin, které mají prvků nekonečně mnoho (např. množina M_2). Takové množiny se nazývají nekonečné, na rozdíl od konečných množin, které mají jen konečně mnoho prvků. Jiný, univerzálnější způsob popisu množiny M spočívá v nalezení takové vlastnosti, kterou mají právě jen všechny prvky dané množiny M. Množinu M tedy popíšeme pomocí výrokové formy $H(x)$, což je, zhruba řečeno, slovní spojení obsahující proměnnou, po jejímž nahrazení objektem z definičního oboru E výrokové formy dostaneme pravdivý či nepravdivý výrok.

Právě ty objekty x definičního oboru E, pro které se $H(x)$ stane pravdivým výrokem, budou prvky množiny M. Píšeme pak $M = \{x: H(x)\}$. Tak můžeme psát $M_3 = \{x: x \in \mathbb{Q} \text{ a } 5x + 3 = -0{,}5\}$, $M_2 = \{x: x \in \mathbb{N}_0 \text{ a } x \text{ je prvočíslo}\}$, $M_4 = \{x: x \in \mathbb{R} \text{ a } x^2 + 9 = 0\}$. Výrokovou formou $H(x)$ můžeme charakterizovat nějakou množinu dokonce i tehdy, když (ještě) nevíme, pro které objekty x definičního oboru je výrok $H(x)$ pravdivý. Tak můžeme např. mluvit o množině $M_9 = \{x: x \text{ je prvočíslo a } 10^{1000} < x < 10^{100\,000}\}$.

Chceme-li charakterizovat množinu M_4 výčtem jejích prvků, zjistíme, že neexistuje žádné reálné číslo, které

by bylo řešením rovnice $x^2 + 9 = 0$, tj. množina M_4 je „prázdná". Množinu, která žádný prvek neobsahuje, nazýváme prázdnou množinou a označujeme ji symbolem $\emptyset$. Vyskytují se mezi množinami M_1 až M_8 ještě další prázdné množiny?

Leží-li prvek x v množině M, píšeme $x \in M$, v opačném případě pak $x \notin M$, např. $3 \in M_1$, $11 \in M_2$, množina $\in$ {množina}, $7 \notin M_7$. Pro označování množin budeme používat velká písmena latinské abecedy A, B, ..., M, ..., X, Y, která budeme případně doplňovat indexem (M_7, B_2). Prvky množin budeme obvykle označovat malými písmeny a, b, ..., x, y, ... (případně též s indexy).

Bez ohledu na uvedené příklady učiníme následující důležitou úmluvu spojenou s pojmem množiny: Každá množina musí být jednoznačně určena svými prvky, tj. svým „obsahem". Množina trampot nemůže tedy být množinou v matematickém smyslu.

Nyní by se mohlo zdát, že se nám už podařilo získat pro další úvahy dostatečně přesnou představu pojmu množina. A přece ne každá vlastnost skutečně jednoznačně určuje množinu. Uvažujme např. vojáka, jenž má holit všechny příslušníky své jednotky, kteří se neholí sami; jak se pak má takový voják zachovat k vlastnímu vousu? Nebo zkusme sestavit „množinu" M všech množin, které nejsou svými vlastními prvky. Lze utvořit takovou množinu?

Obtíže, které vznikají při rozhodování, zda jednotlivé objekty do uvažované množiny patří či nikoliv, spočívají v oblasti logiky. Případ, kdy je množina M zároveň svým vlastním prvkem, musíme vyloučit. My se ale napříště budeme zabývat jen takovými množinami, u kterých se shora uvedené paradoxy nevyskytnou.

Přestože jsme probrali pojem množiny a objasnili ho na příkladech, vyhnuli jsme se tomu podat její přesnou

definici. To u takových základních pojmů, jako je množina nebo bod, také ani nejde; vždyť k tomu bychom potřebovali nějaké ještě jednodušší (a v tomto smyslu základnější) pojmy.

STEJNÉ, NEBO RŮZNÉ?

1.2 ROVNOST MNOŽIN

Podrobněji o rovnosti počtu prvků množin

Uvažujme množiny $A = \{x: x \in \mathbf{R} \text{ a } 2x^2 - 2x - 12 = 0\}$, $B = \{-2; 3\}$ a $C = \{3; -2\}$. Především můžeme zjistit, že každý prvek jedné z množin A, B, C je zároveň prvkem i ostatních dvou (ověřte to!). Množiny A, B, C se tedy liší jen ve svém popisu; mají stejné prvky, stejný obsah. Protože každá množina je jednoznačně určena svými prvky, můžeme definovat:

Definice 1.1. Nechť M_1 a M_2 jsou dvě neprázdné množiny. M_1 a M_2 se nazývají sobě *rovné*, právě když každý prvek množiny M_1 je zároveň prvkem množiny M_2, a naopak — každý prvek M_2 prvkem množiny M_1, tj.
$M_1 = M_2$, právě když pro všechna x platí $x \in M_1 \Leftrightarrow x \in M_2$.
Prázdné množiny se navzájem rovnají.

Pro implikaci „jestliže ... pak" užíváme symbolu $\Rightarrow$, znamená tedy „$x \in M_1 \Rightarrow x \in M_2$" výrok „když $x \in M_1$, pak (také) $x \in M_2$" nebo, jinak řečeno, „z $x \in M_1$ vyplývá $x \in M_2$". Platí-li zároveň $x \in M_1 \Rightarrow x \in M_2$ a také $x \in M_2 \Rightarrow x \in M_1$, píšeme obvykle $x \in M_1 \Leftrightarrow x \in M_2$ (viz také odstavec 2.2).
Nejsou-li množiny M_1 a M_2 sobě rovné, píšeme $M_1 \neq M_2$. Vztah rovnosti, definovaný v D(1.1), má zřejmě

pro libovolné tři množiny M_1, M_2, M_3 následující tři vlastnosti:
(1) Každá množina je rovna sama sobě, tj. platí $M_1 = M_1$.
(2) Z rovnosti $M_1 = M_2$ plyne $M_2 = M_1$.
(3) Z rovnosti $M_1 = M_2$ a $M_2 = M_3$ plyne $M_1 = M_3$.

Při zjišťování, jsou-li dvě množiny A a B sobě rovné, můžeme použít D(1.1) takto: přesvědčíme se, zda pro každý prvek $a \in A$ je také $a \in B$, a obráceně, zda také každý prvek $b \in B$ patří do A.

Množina, která obsahuje pouze jeden prvek, se nazývá jednoprvková; taková je množina M_3 v našem příkladě v odstavci 1.1. Existuje nekonečně mnoho různých jednoprvkových množin, naproti tomu existuje právě jedna prázdná množina. Pro množiny označené v odstavci 1.1 jako M_4 a M_8 platí tedy $M_4 = M_8 = \emptyset$. Také množina $L = \{x: x \neq x\}$ je jen jinak zapsaná prázdná množina, protože neexistuje objekt, který by nebyl sám se sebou identický.

UČITEL JE TAKÉ JENOM ČLOVĚK

1.3 PODMNOŽINY

O vlastních a nevlastních podmnožinách, o potenční množině a o množinách, které nemají žádný společný prvek

Každý ví, co rčení „Učitel je také jenom člověk" vyjadřuje: sotva od něj můžeme čekat něco nadlidského, třeba že by byl vševědoucí nebo neunavitelný. Pro střízlivého matematika vyjadřuje uvedené rčení pouze vztah mezi množinou učitelů a množinou všech lidí. Skutečnost, že každý učitel je člověk, vyjádří takto: Množina učitelů je podmnožinou množiny všech lidí.

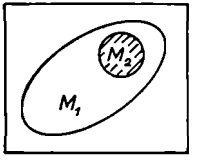
Takovýto vztah „podmnožina — množina“ se objevuje často:

— Množina všech sudých čísel je podmnožinou množiny Z všech celých čísel.
— Množina všech prvočísel je podmnožinou množiny všech přirozených čísel.
— Množina řešení rovnice $4x + 7 = -1$ je podmnožinou řešení nerovnice $2 - 3x > -1$.

Definice 1.2. Nechť M_1 a M_2 jsou množiny. Pak se M_1 nazývá *podmnožinou* M_2 (symbolicky: $M_1 \subset M_2$), právě když každý prvek M_1 patří také do M_2, tj.

$M_1 \subset M_2$, právě když pro každé x platí: $x \in M_1 \Rightarrow x \in M_2$.

Speciálně se M_1 nazývá *vlastní podmnožinou* M_2, právě když platí: $M_1 \subset M_2$ a $M_1 \neq M_2$.



Obr. 1

Vztah být podmnožinou se také nazývá *inkluze*. Na obr. 1 je znázorněno $M_2 \subset M_1$. Všimněte si že symbol $\in$ může stát jen mezi prvkem a množinou, zatímco $\subset$ jen mezi dvěma množinami.

Z D(1.2) získáme několik důsledků:

— Prázdná množina je podmnožinou libovolné množiny M, neboť neexistuje žádné x v $\emptyset$, které by nepatřilo také do M.
— Každá množina je svou podmnožinou.

— Ze vztahu $M_1 \subset M_2$ a $M_2 \subset M_3$ plyne $M_1 \subset M_3$.

Následující věta V(1.1) vyjadřuje vztah mezi rovností a inkluzí.

Věta 1.1. *Pro libovolné dvě množiny M_1 a M_2 platí: $M_1 = M_2$, právě když platí zároveň $M_1 \subset M_2$ i $M_2 \subset M_1$.*

Důkaz věty plyne z D(1.1) a D(1.2).

V následujícím příkladu ukážeme, jak lze využít V(1.1) k důkazu rovnosti dvou množin: chceme dokázat, že množina A všech nezáporných sudých čísel je rovna množině Q všech těch celých nezáporných čísel, jejichž druhá mocnina je sudé číslo.

V prvém kroku ukážeme, že $A \subset Q$: každý prvek $x \in A$ se dá psát ve tvaru $x = 2n$ pro $n \in \mathbb{N}_0$. Z rovnosti $x^2 = (2n)^2 = 2.2n^2$ plyne $x \in Q$, takže $A \subset Q$.

Druhý krok: Nechť $y \in Q$ je libovolné a $y = p_1^{\lambda_1} p_2^{\lambda_2} \ldots$ $\ldots p_n^{\lambda_n}$ $(\lambda_i > 0)$ je jeho rozklad na prvočinitele; ten je až na pořadí určen jednoznačně. Protože podle předpokladu je $y^2 = p_1^{2\lambda_1} p_2^{2\lambda_1} \ldots p_n^{2\lambda_n}$ sudé, musí být jeden z prvočinitelů p_i čísla y^2 roven 2. Je tedy 2 také jeden z prvočinitelů čísla y, a to je tedy sudé. Je tudíž $Q \subset A$. Z obou kroků plyne $A = Q$.

Uvažujme množinu všech podmnožin množiny $B = \{a, b, c\}$ a označme ji $\mathscr{P}(B)$. Je tedy $\mathscr{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Definice 1.3. Budiž M libovolná množina. Množina všech podmnožin množiny M se nazývá *potenční množina množiny M*; budeme ji značit $\mathscr{P}(M)$: $\mathscr{P}(M) = \{X: X \subset M\}$.

Pro libovolnou množinu M jsou $\emptyset$ a M prvky $\mathscr{P}(M)$, je tedy potenční množina množiny M neprázdná.

V shora uvedeném příkladě má B tři prvky, její potenční množina má $2^3 = 8$ prvků. Je-li M jednoprvková, pak zřejmě potenční množina $\mathscr{P}(M)$ obsahuje právě dva prvky $\emptyset$ a M. Potenční množina dvouprvkové množiny $\{a, b\}$ sestává z $2^2 = 4$ prvků $\emptyset$, $\{a\}$, $\{b\}$, $\{a, b\}$.

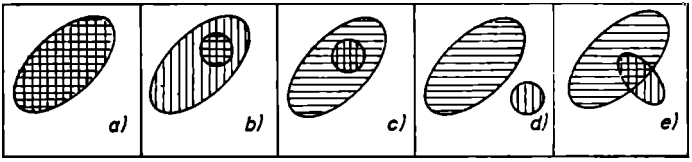
Analýza dosud získaných výsledků nás přivádí k domněnce, že potenční množina n-prvkové množiny má právě 2^n prvků.

K důkazu správnosti naší domněnky použijeme metodu, která bývá označována jako matematická indukce. Tento postup umožňuje dokazovat platnost obecných výroků $H(n)$, které závisejí na parametru $n \in \mathsf{N}_0$: Ukážeme-li v 1. kroku, že dokazovaný výrok H platí pro nějaké počáteční $n_0 \in \mathsf{N}_0$ (často pro 0, 1 nebo 2), a v 2. kroku, že z platnosti $H(k)$ vyplývá platnost $H(k + 1)$, pak platí $H(n)$ pro všechna celá čísla $n \geqq n_0$.

Náš výrok o počtu prvků $\mathscr{P}(M)$ je pro $n = 1$ pravdivý, zbývá tedy provést ještě 2. krok matematické indukce: Předpokládejme, že potenční množina k-prvkové množiny M má 2^k prvků. Přidáme-li k množině M další prvek a_{k+1}, počet prvků $\mathscr{P}(M)$ se zdvojnásobí, neboť ke každé původní podmnožině množiny M přibude ještě odpovídající podmnožina, která z ní vznikne přidáním prvku a_{k+1}. A takto taky dostaneme všechny podmnožiny, protože taková podmnožina buď neobsahuje a_{k+1}, a pak byla podmnožinou i „původní" množiny, nebo obsahuje a_{k+1}, a pak se dá utvořit z jedné z podmnožin „původní" množiny přidáním prvku a_{k+1}. Má tedy potenční množina $(k + 1)$-prvkové množiny $2 . 2^k = 2^{k+1}$ prvků.

Nemají-li dvě množiny A a B společný prvek, nazývají se *disjunktní*. Mají-li A a B aspoň jeden společný prvek a přitom každá z nich obsahuje aspoň jeden další prvek, který v druhé množině neleží, můžeme říci, že se obě množiny navzájem *částečně překrývají*. Jsou-li A, B

dvě neprázdné podmnožiny nějaké množiny M, pak zřejmě nastane vždy právě jedna z následujících pěti možností:
a) $A = B$, b) $A \subset B$ a $A \neq B$, c) $B \subset A$ a $A \neq B$, d) A a B jsou disjunktní, e) A a B se navzájem částečně překrývají (obr. 2).



Obr. 2

PETROVY ŠANCE U HEZKÉ KRISTÝNY — POUHÉ NEDOROZUMĚNÍ?

1.4 MNOŽINOVÉ OPERACE

Čtenář se seznámí s operacemi průniku, sjednocení a rozdílu množin, jakož i s jejich vlastnostmi

Petr vítězoslavně oznamuje svému příteli Wolfgangovi, že má dobré šance u hezké Kristýny, protože podle jejích vlastních slov má obzvlášť ráda sportovní mladíky a kučeravé blonďáky. Wolfgang však ohromeně namítá: „Ale ty máš přece černé vlasy." Tato námitka zas udivuje Petra, který se brání: „Ale zato jsem přece velice sportovní, vždyť na poslední školní tělovýchovné slavnosti jsem získal tři první ceny."

Bohužel nemůžeme rozhodnout, kdo z nich měl více důvodů se divit, protože Kristýna se nevyjádřila jasně.

Následující formulace jsou podobně nepřesné:

(1) Rovnoramenné a pravoúhlé trojúhelníky mají dva úhly velikosti 45°.
(2) Rovnoramenné a pravoúhlé trojúhelníky mají součet úhlů 180°.
(3) Čísla dělitelná čtyřmi a šesti jsou sudá.
(4) Čísla dělitelná čtyřmi a šesti jsou rovněž dělitelná 12.
(5) Monotónní a ohraničené posloupnosti jsou konvergentní.
(6) Monotónní a ohraničené posloupnosti mohou mít nejvýše jednu limitu.

Formulace (1) je výrok o trojúhelnících, které jsou zároveň rovnoramenné a pravoúhlé, zatímco výrok (2) platí pro všechny trojúhelníky, které jsou rovnoramenné nebo pravoúhlé; platí dokonce pro každý trojúhelník. Označuje-li P množinu pravoúhlých a R množinu rovnoramenných trojúhelníků, pak oborem pravdivosti výroku (1) je množina všech prvků, které přísluší jak P, tak R; takovou množinu nazýváme *průnik* P *a* R a píšeme $P \cap R$. Naproti tomu, máme-li na mysli množinu všech těch prvků, které leží aspoň v jedné z množin P nebo R, pak mluvíme o *sjednocení* P *a* R, symbolicky $P \cup R$. Sjednocení $P \cup R$ se tedy skládá z těch prvků, které leží v P, ale neleží v R, z těch, jež leží v R, ale neleží v P, a z těch, které leží v obou množinách P, R. Označíme-li ještě množinu všech prvků, které leží v P, ale neleží v R, jako *rozdíl* $P \setminus R$, pak můžeme psát $P \cup R = (P \setminus R) \cup (R \setminus P) \cup (P \cap R)$, což znázorňuje obr. 3.

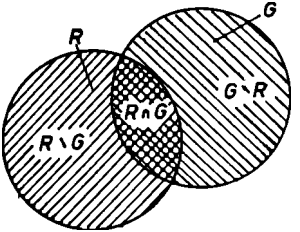
Rozeberte výroky (3) až (6) stejným způsobem.

To, co jsme právě probrali, shrneme v následujících definicích: Nechť $M_1 = \{x: x \in E \text{ a } H_1(x)\}$ a $M_2 = \{x: x \in E \text{ a } H_2(x)\}$ jsou dvě množiny s definičním oborem E.

Definice 1.4. *Průnik množin* M_1 a M_2 je množina $M_1 \cap M_2 = \{x: x \in E \text{ a } (H_1(x) \text{ a zároveň } H_2(x))\}$; tj. $x \in M_1 \cap M_2 \Leftrightarrow (x \in M_1 \text{ a } x \in M_2)$.

Definice 1.5. *Sjednocení množin* M_1 a M_2 je množina
$M_1 \cup M_2 = \{x: x \in E$ a $(H_1(x)$ nebo $H_2(x))\}$;
tj. $x \in M_1 \cup M_2 \Leftrightarrow (x \in M_1$ nebo $x \in M_2)$.

Definice 1.6. *Rozdíl množin* M_1 a M_2 je množina
$M_1 \setminus M_2 = \{x: x \in E$ a $(H_1(x)$ a ne $H_2(x))\}$;
tj. $x \in M_1 \setminus M_2 \Leftrightarrow (x \in M_1$ a $x \notin M_2)$.



Obr. 3

Průnik, sjednocení a rozdíl dvou množin M_1 a M_2 jsou těmito množinami určeny jednoznačně, což je zřejmé také tehdy, jsou-li jedna nebo obě množiny prázdné. Ještě si všimněte, že slovo „nebo" se v definici sjednocení (a v matematice běžně) používá v nevylučujícím smyslu. Na rozdíl od $M_1 \cup M_2$ můžeme množinu těch prvků, které patří buď do M_1, anebo do M_2, popsat jako $(M_1 \cup M_2) \setminus (M_1 \cap M_2)$[2]).

---

[2]) Tato operace se někdy nazývá *symetrický rozdíl množin* M_1 a M_2 a označuje se jako $M_1 \triangle M_2$. Přitom je také $M_1 \triangle M_2 = (M_1 \setminus M_2) \cup (M_2 \setminus M_1)$.
Na tomto místě navíc překladatel vypustil jednu větu, která v češtině ztrácí smysl. Německý výraz pro průnik (Durchschnitt) má totiž ještě další významy (průřez, průměr), a tak je dobře si aspoň uvědomit, jak je slovo průnik výstižné a jedinečné, oč je v tomto směru náš jazyk bohatší (viz též pozn. na str. 7). (Pozn. překl.)

Uvažujme rozdíl $E \setminus M$ základní množiny E a množiny M, tato množina se často nazývá *doplněk množiny M vzhledem k E* a značí se M'_E. Nebude-li hrozit nedorozumění, budeme také tento doplněk označovat stručně M'. Podle D(1.6) je tedy $M'_E = \{x: x \in E \text{ a } x \notin M\}$. Položíme-li ještě $M''_E = (M'_E)'_E$, platí zřejmě $M''_E = M$.

Při popisu matematických souvislostí budeme často používat následující množinové vyjadřování:

— Označuje-li N_0 množinu všech celých nezáporných čísel, M_1, M_2 a M_3 množiny celých nezáporných čísel po řadě dělitelných 2, 3 a 6 a M_4 množinu všech lichých nezáporných čísel, pak je např. $M_1 \cup M_4 = \mathsf{N}_0$, $M_1 \cap M_2 = M_3$, $(M_4)'_{\mathsf{N}_0} = M_1$, $M_2 \cup M_3 = M_2$, $M_2 \cap M_3 = M_3$.

— Průnik dvou různých přímek roviny je buď prázdný, anebo množina, která obsahuje právě jeden bod.

— Množinou řešení soustavy rovnic

$$x + 4y = 3, \tag{1}$$
$$x + y = 0 \tag{2}$$

je průnik množin řešení rovnice (1) a rovnice (2).

— Množinou řešení nerovnice $|x - 1| > 2$ je sjednocení množin řešení nerovnic $x - 1 > 2$ a $x - 1 < -2$.

Z množství vlastností množinových operací shrnujeme v následující větě některé důležité.

Věta 1.2. *Nechť A, B, C jsou libovolné podmnožiny základní množiny E, pak platí následující tvrzení:*

(1) *Vlastnosti průniku a sjednocení*

(1a) $A \cap B = B \cap A$,
(1a′) $A \cup B = B \cup A$,
(1b) $(A \cap B) \cap C = A \cap (B \cap C)$,
(1b′) $(A \cup B) \cup C = A \cup (B \cup C)$,
(1c) $A \cap A = A$,
(1c′) $A \cup A = A$.

(2) *Souvislost průniku a sjednocení*

(2a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
(2a′) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
(2b) $A \cap (A \cup B) = A$,
(2b′) $A \cup (A \cap B) = A$.

(3) *Souvislost průniku a sjednocení s rozdílem*

(3a) $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$,
(3a′) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$,
(3b) $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$,
(3b′) $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

(4) *Souvislost množinových operací s inkluzí*

(4a) $A \cap B \subset A$,
(4a′) $A \subset A \cup B$,
(4b) $A \cap B = A \Leftrightarrow A \subset B$,
(4b′) $A \cup B = A \Leftrightarrow B \subset A$,
(4c) $C \subset A$ a $C \subset B \Rightarrow C \subset A \cap B$,
(4c′) $A \subset C$ a $B \subset C \Rightarrow A \cup B \subset C$,
(4d) $A \subset B \Rightarrow A \setminus C \subset B \setminus C$ a $C \setminus B \subset C \setminus A$.

(5) *Úloha množin $\emptyset$ a E*

(5a) $A \cap \emptyset = \emptyset$,
(5a′) $A \cup E = E$,
(5b) $A \cap E = A$,
(5b′) $A \cup \emptyset = A$,
(5c) $A \cap B = \emptyset \Leftrightarrow B \subset A'$,
(5c′) $A \cup B = E \Leftrightarrow A' \subset B$.

Věta zahrnuje některé speciální případy: dosadíme-li do (3b) a (3b′) $C = E$, dostaneme tzv. *de Morganova*[3]) *pravidla*

[3]) Augustus de Morgan (1806—1871), anglický matematik; zabýval se zejména infinitezimálním počtem, algebrou a pravděpodobností.

$$(A \cap B)' = A' \cup B', \quad (A \cup B)' = A' \cap B'.$$

Podobně dostaneme ze (4d) pro $C = E$ implikaci $A \subset B \Rightarrow B' \subset A'$ a tvrzení (5c) a (5c′) dávají speciálně pro $B = A'$ vztahy $A \cap A' = \emptyset$, $A \cup A' = E$. Čtenář si při pozorném sledování uvedené věty snadno uvědomí zprvu zarážející analogii mezi operacemi „$\cap$“ a „$\cup$“. Ke každému tvrzení je tu také uveden jeho jaksi „zrcadlový obraz“, vyjma ovšem tvrzení (4d), kde se vyskytuje jen rozdíl množin. Tvrzení přejde ve svůj „zrcadlový obraz“, jestliže navzájem zaměníme symboly „$\cap$“ a „$\cup$“ a zároveň množiny $\emptyset$ a E. Přitom se také obrátí případné inkluze, neboť $A \subset B$ je podle (4b) ekvivalentní $A \cap B = A$, a k tomu je „symetrický“ vztah $A \cup B = A$, což je podle (4b′) ekvivalentní $B \subset A$. Matematici tuto dalekosáhlou analogii prozkoumali a obecně dokázali, že s každým tvrzením V(1.2) platí také jeho „zrcadlový obraz“ — říkáme *duální tvrzení*. Kdybychom nechtěli této znalosti využít, museli bychom dokazovat každé z 27 tvrzení V(1.2), zatímco takhle plyne platnost tvrzení (1a′) až (5c′) už z důkazu (1a) až (5c). Ale protože všechny tyto důkazy probíhají podle téhož vzoru, nebudeme zde provádět ani jedno, ani druhé, a místo toho se omezíme na několik příkladů, které dostatečně objasní možné metody důkazu.

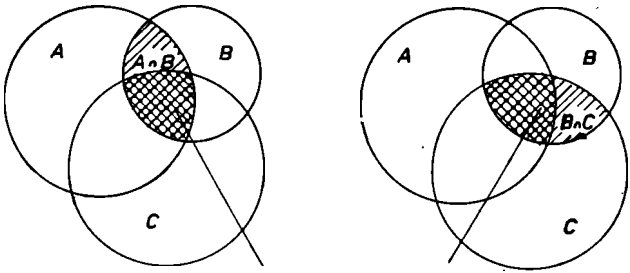
Nejprve však poukažme ještě na to, že tvoření průniku a sjednocení lze rozšířit na systémy $\mathfrak{M}$ více, či dokonce nekonečně mnoha množin: do průniku množin z $\mathfrak{M}$ budou patřit právě ty prvky, které leží v každé množině z $\mathfrak{M}$, a do sjednocení množin z $\mathfrak{M}$ právě ty prvky, které patří alespoň do jedné množiny z $\mathfrak{M}$. Také tvrzení věty (1.2) pak mají smysluplná zobecnění; (1b) můžeme např. vyjádřit ve tvaru „V průniku můžeme libovolně rozmístit či odstranit závorky“ a (3a) pro čtyři

množiny A, B, C, D dostane tvar $(A \cap B \cap C) \setminus D = (A \setminus D) \cap (B \setminus D) \cap (C \setminus D)$.

K důkazu tvrzení (1b) si nejprve uvědomme, že uvedenou rovnost množin $(A \cap B) \cap C = M$ a $A \cap (B \cap C) = N$ dostaneme, potvrdíme-li, že je jak $M \subset N$, tak i $N \subset M$ (srov. odstavec 1.3). Je-li tedy $x \in M$, tj. $x \in (A \cap B) \cap C$, pak platí jak $x \in A \cap B$, tak $x \in C$, odkud dále plyne $x \in A$ a $x \in B$ a $x \in C$. Leží-li x v každé ze tří množin A, B, C, pak je také $x \in A$ a $x \in B \cap C$, tedy $x \in A \cap (B \cap C) = N$. Je tudíž $M \subset N$.

Je-li $x \in N$, tj. $x \in A \cap (B \cap C)$, tak je $x \in A$ a $x \in B \cap C$, odkud opět plyne, že x leží v každé z množin A, B, C. Proto platí $x \in A \cap B$ a $x \in C$, a proto $x \in (A \cap B) \cap C = M$. Je tedy také $N \subset M$, což spolu s $M \subset N$ dává rovnost $M = N$, c. b. d.

Tímto postupem můžeme v zásadě dokázat všechna tvrzení V(1.2); jde v podstatě jen o použití odpovídajících definic. Ať se čtenář sám procvičí na některém z dalších tvrzení uvedených v bodě (1)! Dejte však pozor na to, že množinové diagramy, které se často používají



Obr. 4

k znázornění tvrzení V(1.2), jako např. diagram na obr. 4 pro tvrzení (1b), rozhodně nejsou matematickým důkazem, vždyť znázorňují jen jednu z mnoha možných konstelací mezi množinami A, B, C. Shora uvedená metoda důkazu předpokládá ovšem správné zacházení s logickými operacemi „a" a „nebo".

Jinou možnost nabízí tzv. tabulková metoda, kterou objasníme na důkazu (3a):

A	B	C	$A \cap B$	$(A \cap B) \setminus C$	$A \setminus C$	$B \setminus C$	$(A \setminus C) \cap (B \setminus C)$
1	1	1	1	0	0	0	0
1	1	0	1	1	1	1	1
1	0	1	0	0	0	0	0
1	0	0	0	0	1	0	0
0	1	1	0	0	0	0	0
0	1	0	0	0	0	1	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0

Tabulku chápeme takto: Leží-li prvek x v některé z množin, pak zapíšeme symbol „1", jinak „0". V prvních třech sloupcích jsou probrány všechny možnosti pro příslušnost prvku x ke každé ze tří množin A, B, C. S použitím definic D(1.4) až D(1.6) pak zapisujeme do ostatních sloupců „1" nebo „0". Srovnání pátého a osmého sloupce ukazuje: $x \in (A \cap B) \setminus C$, právě když $x \in (A \setminus C) \cap (B \setminus C)$, c. b. d.

Jako cvičení dokažte pomocí tabulkové metody další dílčí tvrzení V(1.2)!

Někdy lze doporučit metodu nepřímého důkazu, zejména ale u tvrzení uvedených v části (4) V(1.2), ve kterých vstupuje do hry také inkluze: V důkazu (4c') dejme tomu, že existuje prvek $x \in A \cup B$, který neleží v C. Z $x \in A \cup B$ ale plyne, že x patří alespoň do jedné

z obou množin A nebo B. Protože podle předpokladu jsou obě množiny podmnožinou C, plyne odtud také $x \in C$, což je ve sporu s naším předpokladem. Ten je tedy třeba zavrhnout, a platí tedy $A \cup B \subset C$, c. b. d.

Na závěr se vraťme k de Morganovým pravidlům, která bychom pro jejich důležitost měli dokázat, třeba tabulkovou metodou:

A	B	A'	B'	$A \cap B$	$A \cup B$	$(A \cap B)'$	$(A \cup B)'$	$A' \cap B'$	$A' \cup B'$
1	1	0	0	1	1	0	0	0	0
1	0	0	1	0	1	1	0	0	1
0	1	1	0	0	1	1	0	0	1
0	0	1	1	0	0	1	1	1	1

Rovnost sloupců $(A \cap B)'$ a $A' \cup B'$ a sloupců $(A \cup B)'$ a $A' \cap B'$ dává tvrzení, která se měla dokázat.

TVOŘENÍ DVOJIC

1.5 KARTÉZSKÝ SOUČIN

Čtenář se důvěrně seznámí s kartézským součinem množin a jeho vlastnostmi

Petr pozval na oslavu svých narozenin Wolfganga, Rolfa, Uweho a Holgera a také Conny, Ingrid a Aňu. Připravil rychlou taneční hudbu na nejméně pět kol, aby mohl každý chlapec s každou dívkou jednou tančit. Je jeho plán správný?

Napíšeme-li taneční páry ve tvaru (Wolfgang, Aňa), na prvním místě tedy stojí vždy chlapec a na druhém jeho taneční partnerka, utvoříme, matematicky řečeno, *uspořádanou dvojici*. Její *první složka* je prvek množiny A chlapců a její *druhá složka* prvek množiny B děvčat.

Napíšeme-li všechny možné uspořádané dvojice prvků neprázdných množin A a B, dostaneme tak novou množinu $A \times B$ (čti „A krát B"), která se nazývá kartézský součin.

Definice 1.7. Nechť A a B jsou neprázdné množiny.
(1) Každá dvojice (x, y), kde $x \in A$ a $y \in B$, se nazývá *uspořádaná dvojice prvků množin A a B*. Dvě uspořádané dvojice (x_1, y_1) a (x_2, y_2) se rovnají, právě když $x_1 = x_2$ a $y_1 = y_2$.
(2) Množina všech uspořádaných dvojic (x, y), kde $x \in A$ a $y \in B$, se nazývá *kartézský součin $A \times B$ množin A a B*: $A \times B = \{(x, y): x \in A \text{ a } y \in B\}$.

V této definici je rovněž zahrnut často se vyskytující zvláštní případ, když jsou obě množiny A, B stejné ($A = B$). O tento případ se jedná, když např. tvoříme kartézský součin $\mathsf{R} \times \mathsf{R}$, tedy uvažujeme-li množinu všech uspořádaných dvojic reálných čísel. Zavedením souřadnicového systému v rovině můžeme, jak známo, každému bodu této roviny vzájemně jednoznačně přiřadit uspořádanou dvojici (x, y) jeho souřadnic. Teprve toto vzájemně jednoznačné přiřazení mezi body roviny a množinou $\mathsf{R} \times \mathsf{R}$ umožňuje početní řešení geometrických otázek. Tato „analytická geometrie" byla vytvořena René Descartesem (lat. Cartesius[4])); odtud také označení „kartézský součin" pro $A \times B$. Kdybychom se chtěli zabývat analytickou geometrií v trojrozměrném prostoru, tak bychom museli k jednoznačnému označení bodů prostoru použít *uspořádaných trojic* (x_1, x_2, x_3), přičemž $x_1, x_2, x_3 \in \mathsf{R}$. Nehledě na tento speciální pří-

[4]) René Descartes (1596—1650), francouzský filozof a matematik; jeho hlavní matematickou zásluhou je položení základů analytické geometrie.

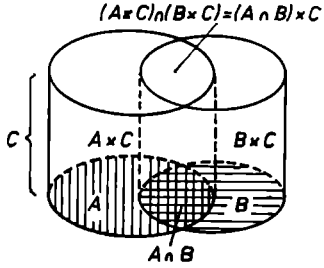
pad, můžeme se přirozeně zabývat pojmem uspořádané trojice (x, y, z) pro libovolné množiny A, B, C, jejichž prvky budou tvořit složky trojice: $x \in A$, $y \in B$, $z \in C$. Také zde je důležité jen to, že dvě takové uspořádané trojice se rovnají, právě když se rovnají po složkách. Množina všech uspořádaných trojic (x, y, z), kde $x \in A$, $y \in B$, $z \in C$, se nazývá *kartézský součin* $A \times B \times C$ *množin* A, B, C.

Analogicky mluvíme o *uspořádané n-tici* $(x_1, x_2, \ldots, x_n)$ prvků množin $A_1, A_2, \ldots, A_n$, když $x_i \in A_i$ pro $i \in \{1, 2, \ldots, n\}$ a když platí, že dvě n-tice se rovnají, právě když se rovnají po složkách. Množina všech uspořádaných n-tic se nazývá *kartézský součin* $A_1 \times A_2 \times \times \ldots \times A_n$ *množin* $A_1, A_2, \ldots, A_n$. Je-li speciálně $A_1 = A_2 = \ldots = A_n = A$, nazývá se $A \times A \times \ldots \times \times A$ často také *n-tá mocnina množiny* A a označuje se A^n. Položíme-li ještě $A^1 = A$, bude symbol A^n definován pro všechny celé kladné exponenty. Protože u uspořádané dvojice podstatně záleží na pořadí prvků, odlišujeme ji od množiny $\{x, y\}$: zatímco je $\{x, y\} = \{y, x\}$, platí $(x, y) \neq (y, x)$, pokud $x \neq y$.

O všech množinách vyskytujících se v našich úvahách se zatím předpokládalo, že jsou neprázdné. Toto omezení můžeme odstranit dodatečnou úmluvou, že $M \times \emptyset = \emptyset \times M = \emptyset$ pro každou množinu M.

Kartézský součin hraje v matematice důležitou úlohu jednak při zavádění tak základních pojmů, jako je relace (srov. kapitolu 2) a zobrazení (srov. odstavec 1.6), jednak při konstrukci nových matematických útvarů. Tak můžeme konstruovat zlomky jako uspořádané dvojice (a, b) celých nezáporných čísel a, b $(b \neq 0)$ tedy prostřednictvím kartézského součinu $\mathsf{N}_0 \times (\mathsf{N}_0 \setminus \setminus \{0\})$; jenom píšeme uspořádanou dvojici (a, b) ve tvaru $\frac{a}{b}$ a říkáme jí zlomek.

Nakonec ještě prozkoumáme, jaká pravidla kartézský součin splňuje. Zřejmě záleží na pořadí činitelů v součinu, neboť obecně je $A \times B \neq B \times A$; vždyť přece uspořádaná dvojice, jejíž první složka je z A a druhá z B, se zpravidla liší od dvojice s první složkou z B a druhou z A. Kromě toho se vícenásobný kartézský součin nedá libovolně uzávorkovat; je $A \times (B \times C) \neq (A \times B) \times C$. Naproti tomu s operacemi průniku, sjednocení a rozdílu snáší se kartézský součin vcelku dobře ve smyslu následující věty V(1.3), kterou je také možno snadno znázornit (obr. 5).



Obr. 5

Věta 1.3. *Pro množiny A, B, C platí:*

(1a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$,
(1b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
(2a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
(2b) $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
(3a) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Důkaz plyne bezprostředně z definic odpovídajících množinových operací; jako příklad dokažme (2a), podle tohoto vzoru probíhají také ostatní důkazy. Rovnost (2a) dvou množin ukážeme jako obvykle:

(1) $(x, y) \in A \times (B \cup C) \Rightarrow x \in A$ a $y \in B \cup C \Rightarrow$
$\Rightarrow x \in A$ a ($y \in B$ nebo $y \in C$) $\Rightarrow (x, y) \in A \times B$ nebo
$(x, y) \in A \times C \Rightarrow (x, y) \in (A \times B) \cup (A \times C)$.
Je tedy $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$.

(2) $(x, y) \in (A \times B) \cup (A \times C) \Rightarrow (x, y) \in A \times B$ nebo
$(x, y) \in A \times C \Rightarrow x \in A$ a ($y \in B$ nebo $y \in C$) $\Rightarrow$
$\Rightarrow x \in A$ a $y \in B \cup C \Rightarrow (x, y) \in A \times (B \cup C)$.
Je tedy také $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$
a z (1) a (2) nyní plyne podle V(1.1) ihned tvrzení (2a), c. b. d.

Další důkazy si proveďte sami.

Stejně snadno se přesvědčíte o správnosti tvrzení

$$A \subset B \Rightarrow A \times C \subset B \times C$$

pro libovolné množiny A, B, C, které můžeme pro $C \neq \emptyset$ obrátit. Dvojnásobné užití tohoto obrácení dává

$$A \times C = B \times C \Rightarrow A = B$$

pro $C \neq \emptyset$. Naše úvahy zůstanou správné, zaměníme-li v uvažovaných kartézských součinech vždy levý a pravý činitel; jen proto, že $C \times A \neq A \times C$, nevyžadují ještě odpovídající pravidla nový důkaz.

KAŽDÝ HRNEC NAJDE SVOU POKLIČKU

1.6 PŘIŘAZENÍ A ZOBRAZENÍ

Čtenář si zopakuje a rozšíří svoje znalosti o binárních relacích, zobrazeních, o prostých zobrazeních stejně jako o inverzních binárních relacích a o skládání binárních relací

V odstavci 1.5 jsme poznali kartézský součin dvou množin. Je-li např. O množina všech obyvatel Lipska

a U množina všech vyučujících na lipských středních školách, skládá se $O \times U$ ze všech uspořádaných dvojic (x, y), kde $x \in O$, $y \in U$. Všeobecně nás však zajímá jen podmnožina tohoto kartézského součinu, a to každá uspořádaná dvojice, pro kterou v určitém okamžiku platí „x je žákem y".

Vyberme z kartézského součinu $L \times L$, kde L označuje množinu všech lidí žijících v určitém daném dnu, podmnožinu všech těch dvojic (x, y), pro něž „x si píše s y", přiřadíme tak každé osobě její partnery při dopisování.

Mezi prvky kartézského součinu $H \times P$ (H je množina všech hrnců, P množina všech pokliček v nějaké kuchyni) kuchařku zajímají jen dvojice (h, p) s vlastností „p se hodí k h". Takové hrnce a pokličky dává dohromady jako „pasující".

Každou podmnožinu F kartézského součinu $M \times N$ nazveme *přiřazení z M do N*[5]; je-li $(x, y) \in F$, nazývá se *y obraz x v přiřazení F* a *x vzor y v přiřazení F*. Nebude-li hrozit nedorozumění, můžeme říkat stručně obraz, resp. vzor.

Při takto zavedeném pojmu přiřazení těžko můžeme čekat, že prvek $x \in M$ bude mít nejvýše jeden obraz, a podobně, že prvek $y \in N$ bude mít nejvýše jeden vzor. Kupříkladu, každý lipský školák má více učitelů a každý lipský učitel více žáků. Má proto smysl uvažovat množinu všech obrazů prvku $x \in M$ v přiřazení F; budeme jí říkat *úplný obraz* v přiřazení F. Analogicky nazveme množinu všech vzorů prvku $y \in N$ v přiřazení F jako *úplný vzor v přiřazení F*. Úplný obraz v přiřazení F

[5]) V české odborné literatuře se téměř výhradně používá termín *binární relace* v množině $M \times N$. Abychom dodrželi posloupnost výkladu a také některé zvláštnosti autorova přístupu, budeme v této kapitole používat místo binární relace termín přiřazení. (Pozn. překl.)

lipského obyvatele x je tedy prázdný, jestliže není žákem, jinak je to množina všech jeho učitelů. Úplný vzor v přiřazení F lipského učitele y je množina jeho žáků. Tento příklad o učitelích a žácích nás upozornil mimo jiné na to, že v přiřazení $F \subset M \times N$ se mohou případně vyskytnout jisté prvky množiny M, které vůbec nejsou vzory v přiřazení F, a zrovna tak je možné, že jisté prvky z N nejsou obrazy v přiřazení F. V našem příkladu vystupují jako vzory jen ti lipští občané, kteří jsou školou povinní; a kojenec zas nemůže být obrazem v přiřazení „x si píše s y".

Proto nazýváme tu podmnožinu množiny M, jež sestává ze všech vzorů v přiřazení F, *definičním oborem* F. Analogicky rozumíme *oborem hodnot* F podmnožinu množiny N všech obrazů v přiřazení F (symbolicky $\mathscr{D}(F)$, $\mathscr{H}(F)$). Je-li F naše přiřazení žák — učitel, zjistíme okamžitě, že $\mathscr{D}(F)$ je množina všech lipských obyvatel školou povinných, $\mathscr{H}(F) = U$. Pro kuchařku je důležitá rovnost $\mathscr{D}(F) = H$, tj. že se ke každému hrnci najde vhodná poklička.

V následující definici jsou shrnuty všechny právě zavedené pojmy.

Definice 1.8. (1) *Přiřazení F z množiny M do množiny N* je podmnožina kartézského součinu $M \times N$:
F je přiřazení z M do $N \Leftrightarrow F \subset M \times N$.
Místo „F je přiřazení z M do N" píšeme stručně F: $M \to N$.

(2) Je-li $(x, y) \in F$, nazývá se *y obraz prvku x v přiřazení F*, x se nazývá *vzor prvku y v přiřazení F*. Říkáme, že F přiřazuje prvku x prvek y a píšeme též $x \overset{F}{\mapsto} y$.

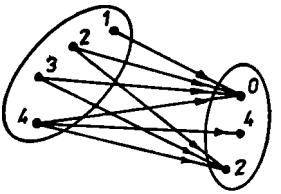
(3) Množina všech obrazů při F prvku $x \in M$ se nazývá *úplný obraz x v přiřazení F*; množina všech vzorů v přiřazení F prvku $y \in N$ se nazývá *úplný vzor y v přiřazení F*.

(4) Množina všech vzorů v přiřazení F se nazývá *definiční obor* $\mathscr{D}(F)$ *přiřazení* F; množina všech obrazů v přiřazení F se nazývá *obor hodnot* $\mathscr{H}(F)$ *přiřazení* F.

Protože přiřazení jsou podle D(1.8) množiny, je také jasné, kdy se dvě přiřazení F a G z M do N rovnají:

$F = G$, právě když pro všechna $x \in M$, $y \in N$ platí: $(x, y) \in F \Leftrightarrow (x, y) \in G$.

Z tohoto množinově teoretického přístupu také hned vyplývají možnosti, jak přiřazení F: $M \to N$ popsat; buď provedeme výčet všech dvojic $(x, y) \in M \times N$ příslušných k F, nebo udáme charakteristickou vlastnost, kterou mají právě jen dvojice kartézského součinu $M \times N$ patřící do F.

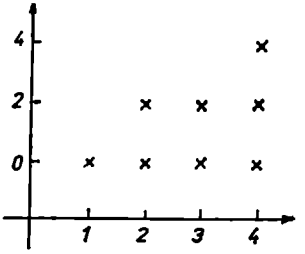


Obr. 6

Pro znázornění přiřazení F: $M \to N$ přiřaďme každému prvku $x \in M$ a každému $y \in N$ právě jeden bod P_x, resp. P_y, v rovině. Různým prvkům přiřadíme různé body, nejpřehledněji tak, že všechny body přiřazené prvkům z M budou ležet v jedné oblasti roviny a body přiřazené prvkům z N v jiné, s prvou disjunktní oblasti téže roviny, jak je patrné z obr. 6. Pak nakreslíme šipku z bodu P_x do bodu P_y, právě když platí $(x, y) \in F$. Vznikne tak uzlový graf přiřazení F. Přirozeně se dá takto přiřazení F plně zobrazit, jen když jsou $\mathscr{D}(F)$ a $\mathscr{H}(F)$ konečné množiny. Např. pro $M = \{1, 2, 3, 4\}$,

$N = \{0, 2, 4\}$ a $F = \{(1; 0), (2; 0), (2; 2), (3; 0), (3; 2), (4; 0), (4; 2), (4; 4)\}$ ukazuje uzlový graf přiřazení F obr. 6.

K další možnosti znázornění se nechámc inspirovat známým zobrazováním funkcí v souřadnicovém systému: Nakreslíme dvě (pro jednoduchost navzájem kolmé) souřadnicové osy, na jedné z os zvolíme body odpovídající prvkům z M (různým prvkům odpovídají různé body, a obráceně), na druhé ose body odpovídající prvkům z N a v souřadnicové rovině označíme právě ty body se souřadnicemi x, y, pro něž platí $(x, y) \in F$. Tak dostaneme graf přiřazení. Graf předchozího příkladu je na obr. 7.



Obr. 7

Pro každé přiřazení F z M do N je $\mathscr{D}(F) \subset M, \mathscr{H}(F) \subset N$. Speciální případy $\mathscr{D}(F) = M$, resp. $\mathscr{H}(F) = N$ budeme odlišovat i slovně: V případě $\mathscr{D}(F) = M$ budeme mluvit o *přiřazení M do N*, v případě $\mathscr{H}(F) = N$ o *přiřazení z M na N*. Dostáváme tak pro přiřazení F: $M \to N$ čtyři případy, které shrnuje následující tabulka.

	$\mathscr{H}(F) \subset N$, $\mathscr{H}(F) \neq N$	$\mathscr{H}(F) = N$
$\mathscr{D}(F) \subset M$, $\mathscr{D}(F) \neq M$	F je přiřazení z M do N	F je přiřazení z M na N
$\mathscr{D}(F) = M$	F je přiřazení M do N	F je přiřazení M na N

Proberme ještě několik příkladů přiřazení:

(1) Je-li K daná kružnice, nechť je každému bodu P roviny, který neleží uvnitř kružnice, přiřazen bod P' dotyku tečny sestrojené z bodu P ke kružnici K. Označíme-li M množinu všech bodů roviny, dostáváme tak přiřazení F z M do M a platí: $(P, P') \in F$, právě když PP' je tečna ke K s bodem dotyku P'. Je tedy $\mathscr{D}(F)$ množina všech bodů neležících uvnitř kružnice K, $\mathscr{H}(F)$ je množina všech bodů kružnice. Úplný obraz v přiřazení F bodu P sestává ze dvou bodů (právě z jednoho bodu), leží-li P vně K (na K). Úplný vzor v přiřazení F bodu P' kružnice K je množina všech bodů tečny sestrojené ke K v bodě P'.

(2) Nechť přiřazení F přiřadí každému reálnému číslu x jeho druhou mocninu x^2. Pak je F přiřazení R do R, přesněji R na R_0^+, kde R_0^+ označuje množinu všech nezáporných reálných čísel. Úplný obraz v přiřazení F každého prvku $x \in \mathsf{R}$ obsahuje právě jeden prvek. Úplný vzor v přiřazení F prvku $y \in \mathsf{R}$ je prázdný, jestliže $y < 0$, obsahuje právě jeden prvek, je-li $y = 0$, a obsahuje právě dva prvky, jestliže $y > 0$.

(3) Přiřazení F: $M \to M$, pro něž $(x, y) \in F$, právě když $x = y$, tj. které zobrazuje každý prvek množiny M na sebe, se nazývá *identické přiřazení* I_M.

(4) Přiřazení F: $M \to N$, pro něž $(x, c) \in F$ pro všechna $x \in M$ a pro pevné $c \in N$, které každému prvku

$x \in M$ přiřazuje tentýž prvek $c \in N$, se nazývá *konstantní přiřazení*.

(5) Přiřazení P_x: $M \times N \to M$, které každé uspořádané dvojici $(x, y) \in M \times N$ přiřazuje její první složku x, se nazývá *projekce* $M \times N$ *na* M. Toto označení bude hned srozumitelné, jestliže toto přiřazení znázorníme geometricky v souřadnicovém systému. Zde je $\mathscr{D}(F) = M \times N, \mathscr{H}(F) = M$, P_x je tedy přiřazení $M \times N$ na M. Analogicky se nazývá přiřazení P_y: $M \times N \to N$, kde $P_y = \{((x, y), y): x \in M, y \in N\}$, *projekce* $M \times N$ *na* N, neboť přiřazuje každé uspořádané dvojici (x, y) její druhou složku y.

Je-li F: $M \to N$ přiřazení z M do N, můžeme se ptát po přiřazení, které přiřazení F „obrací", jež tedy každému obrazu $y \in N$ v přiřazení F přiřadí opět jeho vzory z M, jeho úplný vzor v přiřazení F. Toto přiřazení z N do M se bude nazývat *inverzní přiřazení k* F a budeme ho značit F^{-1}.

Definice 1.9. *Inverzním přiřazením* F^{-1} *k přiřazení* F: $M \to N$ budeme rozumět přiřazení F^{-1}: $N \to M$, kde $F^{-1} = \{(y, x): (x, y) \in F\}$, tj. F^{-1} obsahuje uspořádanou dvojici (y, x), právě když je $(x, y) \in F$.

Z této definice okamžitě plyne:

— Jestliže $(x, y) \in F$, je úplný obraz prvku x v přiřazení F roven úplnému vzoru x v přiřazení F^{-1} a úplný vzor v přiřazení F je roven úplnému obrazu y v přiřazení F^{-1}.

— $\mathscr{D}(F^{-1}) = \mathscr{H}(F); \mathscr{H}(F^{-1}) = \mathscr{D}(F)$.

— Přiřazení $(F^{-1})^{-1}$ inverzní k F^{-1} je rovno původnímu přiřazení F, neboť
$(F^{-1})^{-1} = \{(x, y): (y, x) \in F^{-1}\} = \{(x, y): (x, y) \in F\} = F$.

Inverzní přiřazení k přiřazení z příkladu 2 je tedy to,

které každému nezápornému reálnému číslu y přiřazuje obě čísla $+\sqrt{y}$ a $-\sqrt{y}$.

Pro aplikace jsou zvlášť důležitá taková přiřazení F, která každému prvku $x \in \mathscr{D}(F)$ přiřazují právě jeden obraz $y \in \mathscr{H}(F)$. Taková přiřazení, jako např. přiřazení z příkladu 2, se nazývají *zobrazení* nebo *funkce*[6]) a obraz x v přiřazení F se označuje jako $F(x)$.

Je zvykem označovat funkce malými písmeny latinské nebo řecké abecedy pro lepší odlišení od obecných přiřazení — zejména písmeny f, g, h, φ, ψ, ϱ, σ, τ, π; např. i se používá pro identické zobrazení. Příklad 2 ukazuje, že inverzní přiřazení k zobrazení F už nemusí být zobrazením. Zobrazením je tehdy a jen tehdy, jestliže také pro každé $y \in \mathscr{H}(F)$ úplný vzor y obsahuje právě jeden prvek $x \in \mathscr{D}(F)$, tj. když nejen vzor jednoznačně určuje svůj obraz, ale také obraz dovoluje jednoznačně určit svůj vzor. Taková přiřazení se nazývají *vzájemně jednoznačná zobrazení* (někdy také jednojednoznačná). Právě zdvojení slova „jedno" má naznačit, že přiřazení je „jednoznačné v obou směrech". Příkladem pro to je zobrazení $f\colon \mathsf{R} \to \mathsf{R}$, $f = \{(x, x^3)\colon x \in \mathsf{R}\}$. Místo toho obvykle píšeme stručně $f(x) = x^3$, neboť předpis, který každému $x \in \mathscr{D}(f)$ jednoznačně přiřazuje jeho obraz $y = x^3 \in \mathscr{H}(f)$, může být zprostředkován pomocí početního výrazu nazývaného také funkční předpis. Přesto ale musíme navzájem přísně rozlišovat funkci f a její funkční předpis, např. $y = f(x)$; je

$$f = \{(x, y)\colon x \in \mathscr{D}(f) \text{ a } y = f(x)\}.$$

Kromě toho bychom mohli tutéž funkci charakterizovat různými početními výrazy, např. $f = \{(x, y)\colon x \in \mathsf{N}_0 \text{ a } y = (-1)^x\} = \left\{(x, y)\colon x \in \mathsf{N}_0 \text{ a } y = \sin\left(\pi x + \frac{\pi}{2}\right)\right\}$.

[6]) Funkcemi nazýváme ta zobrazení, jejichž obor hodnot je číselná množina. (Pozn. překl.)

Také musíme přísně rozlišovat mezi obrazem $f(x)$ prvku x — zde je x libovolný pevný prvek z $\mathscr{D}(f)$ — a pravou stranou $f(x)$ funkčního předpisu, ve kterém x značí proměnnou s definičním oborem $\mathscr{D}(f)$. Upozorňujeme na to hlavně proto, že pro oboje používáme stejný symbol. Je-li f vzájemně jednoznačné zobrazení, je také f^{-1} vzájemně jednoznačné, což okamžitě odvodíte ze vztahu $(F^{-1})^{-1} = F$, který je správný pro libovolné přiřazení F.

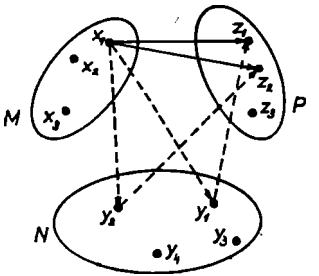
Definice 1.10. (1) Přiřazení F: $M \to N$ se nazývá *zobrazení* nebo *funkce*, právě když pro všechna $x \in \mathscr{D}(F)$, $y_1, y_2 \in \mathscr{H}(F)$ platí:
$[(x, y_1) \in F \text{ a } (x, y_2) \in F] \Rightarrow y_1 = y_2$;
jinak řečeno: různé obrazy mají také různé vzory.
(2) Přiřazení F: $M \to N$ se nazývá *vzájemně jednoznačné zobrazení*, právě když je to zobrazení a pro všechna $x_1, x_2 \in \mathscr{D}(F)$, $y \in \mathscr{H}(F)$ platí:
$[(x_1, y) \in F \text{ a } (x_2, y) \in F] \Rightarrow x_1 = x_2$;
jinak řečeno: různé obrazy mají různé vzory a různé vzory mají také různé obrazy.

Na závěr se ještě podívejme na skládání přiřazení, operaci nám už dobře známou pro funkce.

Definice 1.11. Jsou-li F: $M \to N$ a G: $N \to P$ dvě přiřazení, pak jejich *součinem* nebo *složením* $F \circ G$ (čteme „F složeno s G“) rozumíme takové přiřazení z M do P, pro něž je $F \circ G = \{(x, z)$: existuje y, že $(x, y) \in F$ a $(y, z) \in G\}$.

Zvlášť názornou představu o skládání dvou přiřazení nám zprostředkovává uzlový graf (obr. 8). Ten vznikne „přemostěním“ všech na sebe navazujících dvojic šipek patřících do F a do G, bezprostředně tak spojíme prvek

z M s prvkem z P. Nakonec je také prospěšné si rozmyslet, jak se pozná zobrazení (resp. vzájemně jednoznačné zobrazení) podle uzlového nebo kartézského grafu.



Obr. 8

Jsou-li funkce f a g dány funkčními předpisy $y = f(x)$, resp. $y = g(x)$, přísluší funkci $f \circ g$ funkční předpis $y = g(f(x))$; platí tedy: $[f \circ g](x) = g(f(x))$ pro všechna $x \in \mathscr{D}(f \circ g) \subset \mathscr{D}(f)$. Může se ovšem také stát, že je $f \circ g = \emptyset$, je-li totiž $\mathscr{H}(f) \cap \mathscr{D}(g) = \emptyset$.

Je-li F přiřazení z M do M, pak můžeme také utvořit $F \circ F$. Např. pro $F = \left\{(x, y): x \in \mathsf{R} \setminus \{0\} \text{ a } y = \frac{1}{x}\right\}$ je součin $F \circ F = I_{\mathscr{D}(F)}$ (identita na $\mathscr{D}(F)$.) Přiřazení $F \neq I$ s vlastností $F \circ F = I_{\mathscr{D}(F)}$ se nazývají *involuce*; dvojnásobné užití involuce F na prvek $x \in \mathscr{D}(F)$ dává tedy opět tento prvek x. Také osová souměrnost podle přímky v rovině je involuce.

O postupném skládání přiřazení můžeme vyslovit následující větu:

Věta 1.4. (1) *Vícenásobné složení přiřazení je možno*

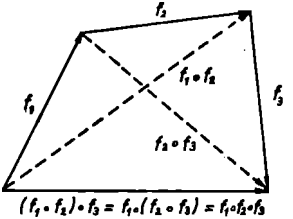
libovolně uzávorkovat: $F_1 \circ (F_2 \circ F_3) = (F_1 \circ F_2) \circ F_3$.

(2) *Pořadí jednotlivých činitelů v součinu přiřazení je podstatné; obecně platí* $F \circ G \neq G \circ F$.

(3) $(F \circ G)^{-1} = G^{-1} \circ F^{-1}$ *pro libovolná přiřazení* F, G.

(4) *F, G jsou (vzájemně jednoznačná) zobrazení* $\Rightarrow$ *$F \circ G$ je (vzájemně jednoznačné) zobrazení.*

Důkaz. (1) Je-li $(x, u) \in F_1 \circ (F_2 \circ F_3)$, existuje podle definice D(1.11) y, pro něž $(x, y) \in F_1$ a $(y, u) \in F_2 \circ F_3$; z posledního vztahu plyne opět existence z, že $(y, z) \in F_2$ a $(z, u) \in F_3$. Pak je ale $(x, z) \in F_1 \circ F_2$ a $(z, u) \in F_3$, tedy $(x, u) \in (F_1 \circ F_2) \circ F_3$. Platí tedy $F_1 \circ (F_2 \circ F_3) \subset \subset (F_1 \circ F_2) \circ F_3$ a stejně se ukáže i obrácená inkluze (obr. 9 to ilustruje pro tři funkce f_1, f_2, f_3).



Obr. 9

(2) Je-li $F: M \to N$, $G: N \to P$, je sice $F \circ G$ přiřazení z M do P, ale $G \circ F$ nelze obecně vůbec utvořit (když $M \cap P = \emptyset$). Ale i když existují obě přiřazení $F \circ G$ i $G \circ F$, jsou zpravidla navzájem různá, jak je vidět už na reálných funkcích s předpisy $f(x) = x^2$ a $g(x) = \sin x$: $[f \circ g](x) = \sin x^2$, ale $[g \circ f](x) = (\sin x)^2 = \sin^2 x$.

(3) Je-li $(z, x) \in (F \circ G)^{-1}$, je podle definice inverzního přiřazení $(x, z) \in F \circ G$; existuje tudíž y, pro které

$(x, y) \in F$ a $(y, z) \in G$. Pak je ale $(y, x) \in F^{-1}$ a $(z, y) \in G^{-1}$, a tedy $(z, x) \in G^{-1} \circ F^{-1}$. Máme tudíž $(F \circ G)^{-1} \subset G^{-1} \circ F^{-1}$, a stejně se ukáže obrácená inkluze.

(4) Pro jednoznačnost $F \circ G$ je potřeba ukázat: $Z(x, z_1) \in F \circ G$ a $(x, z_2) \in F \circ G$ plyne $z_1 = z_2$. Protože $(x, z_1) \in F \circ G$, existuje prvek y_1, pro který $(x, y_1) \in F$ a $(y_1, z_1) \in G$, a protože $(x, z_2) \in F \circ G$, existuje prvek y_2, pro který $(x, y_2) \in F$ a $(y_2, z_2) \in G$. Ze vztahů $(x, y_1) \in F$ a $(x, y_2) \in F$ však vzhledem k jednoznačnosti F plyne, že je $y_1 = y_2 = y$. Pak ale máme $(y, z_1) \in G$ a $(y, z_2) \in G$ a z jednoznačnosti G dostáváme $z_1 = z_2$. Je tedy $F \circ G$ jednoznačné. Jsou-li F a G dokonce vzájemně jednoznačná, jsou zejména F, G, F^{-1}, G^{-1} vesměs jednoznačná. Podle toho, co jsme právě dokázali, jsou pak také součiny $F \circ G$ a $G^{-1} \circ F^{-1} = (F \circ G)^{-1}$ jednoznačná přiřazení. A proto je tedy $F \circ G$ vzájemně jednoznačné zobrazení.

STRÝC TEODOR POŘIZUJE ZÁVĚŤ

1.7 ROZKLAD MNOŽINY NA TŘÍDY

Zde objasníme, kdy se rozdělení množiny na podmnožiny nazývá rozkladem této množiny na třídy

Klaus referuje svému příteli Petrovi: „Nedávno chtěl Werner při vyučování rozdělit všechny trojúhelníky na pravoúhlé a rovnoramenné. Náš učitel byl sice rád, že Werner vůbec pochopil dva matematické pojmy, my jsme však zas jednou měli zábavu."

Čtenář jistě chápe Klausovu veselost, a my se proto zdržíme komentáře. Tak jako chtěl Werner disjunktně rozdělit trojúhelníky, tak strýc Teodor pečlivě postupuje při psaní své závěti, neboť chce zabránit zbytečným dědickým sporům. Chtěl by proto rozdělit veškeré

své jmění tak, aby při podělení dědiců žádná věc nezůstala opomenuta, ale aby také nic nepřipadlo více dědicům. Krom toho nemá být vynechán žádný zákonitý dědic. Budou-li pak dědicové respektovat jeho poslední vůli, nevzniknou žádné rozmíšky kvůli rozdělení majetku.

To nás vede ke zkoumání podmínek, které musí splňovat *rozklad množiny M na podmnožiny*, jež se pak nazývají *třídy*. Nejprve přirozeně musíme dbát na to, aby každý prvek množiny M příslušel některé třídě, tj. aby rozklad množiny M na třídy zahrnoval všechny prvky. To si ovšem strýc Teodor uvědomoval. Naproti tomu rozdělení celých čísel Z na celá kladná a celá záporná čísla nemůžeme akceptovat jako rozklad množiny Z, neboť číslo 0 by zůstalo opomenuto.

Také rozdělení čtyřúhelníků na rovnoběžníky, kosočtverce, deltoidy a na čtyřúhelníky se čtyřmi různě dlouhými stranami je vskutku pochybené, neboť kupříkladu nevíme, zda čtverce počítat mezi rovnoběžníky nebo kosočtverce, anebo mezi deltoidy. Chtěli bychom samozřejmě o každém prvku rozkládané množiny přece přesně vědět, do které třídy rozkladu padne; tak jako se strýc Teodor stará o to, aby žádná část pozůstalosti nepřipadla více dědicům. Tento požadavek zřejmě splníme pochopitelnou podmínkou, aby každé dvě různé třídy byly vždy disjunktní.

A konečně asi nikoho nenapadne utvořit více navzájem disjunktních tříd, než je k sestrojení rozkladu nezbytně nutné; nebudeme tedy dělit množinu modrých, červených, zelených a žlutých předmětů podle barvy do pěti nebo více tříd, když by pak přirozeně zůstala nejméně jedna třída prázdná. Budeme tedy celkem rozumně požadovat, aby žádná ze tříd rozkladu množiny M nebyla prázdná.

Vzhledem k tomu, že třídy rozkladu M jsou podmnoži-

ny M, čili množina všech tříd rozkladu je tudíž podmnožinou potenční množiny $\mathscr{P}(M)$ množiny M, můžeme nyní definovat pojem „rozkladu M“.

Definice 1.12. Jsou-li K_i podmnožiny množiny M ($i = 1, 2, 3, \ldots$; případně i nekonečně mnoho), nazývá se množina $\mathfrak{Z} = \{K_i\}$ všech těchto podmnožin *rozklad množiny M na třídy*, právě když současně platí:
(1) Každé $x \in M$ náleží jen do jedné z množin K_i.
(2) Libovolné dvě z těchto podmnožin jsou si buď rovny, nebo jsou disjunktní:
$K_i \neq K_j \Rightarrow K_i \cap K_j = \emptyset$.
(3) Žádná z podmnožin není prázdná: $K_i \neq \emptyset$ pro všechna i.
Podmnožiny K_i ze $\mathfrak{Z}$ se pak nazývají *třídy rozkladu $\mathfrak{Z}$ množiny M*.

Podívejme se teď na několik příkladů takových rozkladů:

(1) Při konstrukci zlomků vyjdeme z množiny všech uspořádaných dvojic (a, b) celých nezáporných čísel $a, b, b \neq 0$, místo (a, b) píšeme ovšem obvykle $\frac{a}{b}$. Nyní zařadíme každý zlomek $\frac{a}{b}$ do třídy $K\left(\frac{a}{b}\right)$ takovýchto zlomků předpisem: $\frac{c}{d} \in K\left(\frac{a}{b}\right)$, právě když $ad = bc$. Např. třída $K\left(\frac{3}{9}\right)$ kromě jiných obsahuje zlomky $\frac{1}{3}, \frac{2}{6}, \frac{3}{9}, \frac{15}{45}, \frac{113}{339}$.
Přesvědčme se, že takto dostaneme rozklad množiny všech nezáporných zlomků na třídy.

(a) Libovolný zlomek $\frac{a}{b}$ padne alespoň do jedné z uva-

žovaných tříd, totiž do třídy $K\left(\frac{a}{b}\right)$, neboť $\frac{a}{b} \in K\left(\frac{a}{b}\right)$ díky rovnosti $ab = ab$.

(b) Jsou-li $K\left(\frac{a}{b}\right)$ a $K\left(\frac{c}{d}\right)$ různé třídy, pak jsou disjunktní, což nejsnáze ukážeme nepřímo: Kdyby zlomek $\frac{x}{y}$ ležel v obou třídách, a tedy i v jejich průniku, plynulo by z $\frac{x}{y} \in K\left(\frac{a}{b}\right)$, že $ay = bx$, a analogicky bychom dostali $cy = dx$ ze vztahu $\frac{x}{y} \in K\left(\frac{c}{d}\right)$.

Implikace

$$\left.\begin{array}{l} ay = bx \Rightarrow ayd = bxd \\ cy = dx \Rightarrow cyb = dxb \end{array}\right\} \Rightarrow ayd = cyb \Rightarrow ad = bc$$

dávají $ad = bc$, odkud, jak hned uvidíme, plyne naopak rovnost obou tříd. Je-li totiž $\frac{a'}{b'}$ nějaký prvek $K\left(\frac{a}{b}\right)$, tj. $ab' = a'b$, pak také platí $a'bd = ab'd = b'(ad) = b'(bc)$, odkud vzhledem k tomu, že $b \neq 0$, plyne $a'd = b'c$, což ale znamená, že $\frac{a'}{b'} \in K\left(\frac{c}{d}\right)$. Je tedy $K\left(\frac{a}{b}\right) \subset K\left(\frac{c}{d}\right)$, a stejným způsobem se ukáže, že $K\left(\frac{c}{d}\right) \subset K\left(\frac{a}{b}\right)$; napište si tuto část důkazu! Je tudíž $K\left(\frac{a}{b}\right) = K\left(\frac{c}{d}\right)$.

(c) Žádná ze tříd není prázdná, neboť $K\left(\frac{a}{b}\right)$ obsahuje, jak jsme už ukázali v (a), přinejmenším zlomek $\frac{a}{b}$.

Dostali jsme tak rozklad množiny všech (nezáporných) zlomků na „třídy zlomků se stejným podílem", což už jistě znáte. Každá taková třída se nazývá *racionální číslo*.

(2) Rozložíme množinu $\mathbf{Z}$ celých čísel na tři třídy K_0, K_1 a K_2 podle následujícího principu: Třída K_0 bude obsahovat právě čísla dělitelná třemi, K_1 (resp. K_2) bude obsahovat každé celé číslo, které při dělení třemi dá zbytek 1 (resp. 2). Dvě celá čísla, která dají při dělení třemi tentýž zbytek, se nazývají *kongruentní modulo* 3 a píšeme $a \equiv b \pmod 3$. Např. je $623 \equiv 263 \pmod 3$, ale $624 \not\equiv 263 \pmod 3$, přičemž $\not\equiv$ chápeme a čteme jako „není kongruentní modulo 3". Jak vypadají třídy uvedeného rozkladu?

$$K_0 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \{3n : n \in \mathbf{Z}\},$$
$$K_1 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} = \{3n + 1 : n \in \mathbf{Z}\},$$
$$K_2 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} = \{3n + 2 : n \in \mathbf{Z}\}.$$

Vlastně nejsme ještě vůbec oprávněni mluvit o třídách, i když se to zdá být zřejmé. Ověřme to tedy ještě:
(a) Každé celé číslo patří do jedné třídy, totiž do třídy K_i, jestliže dává při dělení třemi zbytek i. Protože jsou možné jenom zbytky 0, 1 nebo 2, leží v K_0, K_1 nebo K_2.
(b) Dvě různé třídy K_i a K_j jsou disjunktní, protože nezáporný zbytek (menší než 3), který dostaneme při dělení třemi, je určen jednoznačně, neexistuje celé číslo, které by při dělení třemi dávalo jak zbytek i, tak také zbytek $j \neq i$.
(c) Žádná třída není prázdná; např. je $0 \in K_0$, $1 \in K_1$, $2 \in K_2$. Třídy tohoto rozkladu se celkem pochopitelně nazývají *zbytkové třídy modulo* 3; přirozeně můžeme $\mathbf{Z}$

rozložit také na 6 zbytkových tříd modulo 6, na 529 zbytkových tříd modulo 529, obecně na m tříd modulo m ($m \geqq 2$). Zbytkové třídy hrají v matematice důležitou úlohu např. v teorii čísel. V následujícím textu budeme obecné souvislosti také často vysvětlovat na příkladu zbytkových tříd.

(3) Rozložení definičního oboru funkce f na třídy prvků se stejným obrazem, tj. na úplné vzory prvků z oboru hodnot, je rozklad; třídy tohoto rozkladu se nazývají *řezy funkce* a definují se jako $K_y = \{z \in \mathscr{D}(f): (z, y) \in f\}$.
(a) Každý prvek $x \in \mathscr{D}(f)$ přísluší alespoň jedné třídě, neboť vzhledem k tomu, že $x \in \mathscr{D}(f)$, obsahuje f alespoň jednu dvojici s první složkou x: $(x, y) \in f$. Je tedy $x \in K_y$.
(b) Libovolné dvě třídy $K_y \neq K_z$ jsou disjunktní, protože kdyby bylo $x \in K_y$ a $x \in K_z$, tak by bylo $(x, y) \in f$ a $(x, z) \in f$, odkud díky jednoznačnosti f okamžitě plyne $y = z$, tedy $K_y = K_z$, což je spor s předpokladem $K_y \neq K_z$.
(c) Žádná třída není prázdná, neboť každý obraz při f obsahuje alespoň jeden vzor.
Tak funkci s funkčním předpisem $y = \sin x$ přísluší obrazu $y = 0$ řez $K_0 = \{\ldots, -2\pi, -\pi, 0, \pi, 2\pi, \ldots\} = \{k\pi: k \in \mathbf{Z}\}$; obrazu $y = s$ ($-1 \leqq s \leqq 1$) přísluší jako řez K_s množina prvních souřadnic všech průsečíků přímky $y = s$ s grafem funkce sinus. Máme-li při řešení goniometrické nebo trigonometrické úlohy vyčíslit hledaný úhel z hodnoty goniometrické funkce, máme-li jej tedy „přečíst" z tabulky této funkce, vezmeme podle našeho způsobu vyjadřování z tabulky prvek řezu. Všechna řešení goniometrické rovnice pak dostaneme, přihlédneme-li ke vztahům mezi kvadranty a k periodicitě funkce.

(4) Podíváme se ještě na jeden zajímavý příklad rozkladu množiny, jejíž prvky jsou opět množiny: V po-

tenční množině $\mathscr{P}(\mathsf{R})$ množiny R reálných čísel zařadíme množiny $A, B \in \mathscr{P}(\mathsf{R})$ do téže třídy, právě když existuje vzájemně jednoznačné zobrazení A na B. Jsou-li množiny A a B konečné, pak je k tomu zřejmě nutné a stačí, aby obě měly stejný počet prvků. V oboru konečných podmnožin potenční množiny tento předpis tedy vede k rozdělení množin podle počtu jejich prvků, a to je jistě rozklad podle naší definice. Jestliže ale vstoupí do hry také nekonečné množiny, je třeba ještě ukázat, zda i pak dostaneme rozklad. Jaké třídy vzhledem k uvedenému rozkladu pak ještě vzniknou, prozradíme v odstavci 1.8.

Spolu s těmito příklady vznikají takovéto otázky: Je možné každý rozklad množiny M vytvořit nějakým takovým předpisem, tj. vztahem, který určuje, kdy dva prvky z M patří do téže třídy a kdy ne?

Jaké má mít takový vztah mezi prvky množiny M vlastnosti, aby vznikl rozklad M?

Těmto otázkám se budeme věnovat v odstavci 2.3.

JE ČÁST MENŠÍ NEŽ CELEK?

1.8 POJEM MOHUTNOSTI
Zajímavě o nekonečných množinách

Jsou-li hosté pozváni na oslavu narozenin, je takřka samozřejmé, že každý dostane díl slavnostního dortu a že každý díl je menší než celý dort.

Při výrocích o množinách chtěli bychom „část celku" přeložit jako „vlastní podmnožina množiny". Učiníme nyní zajímavý objev, že tvrzení „část je menší než celek" musí sice vždy platit pro konečné množiny, ale ne nutně pro nekonečné množiny.

Je-li v kině každé sedadlo obsazené, má množina

diváků právě tolik prvků jako množina v kině se vyskytujících sedadel. To víme, aniž bychom museli sedadla a diváky počítat. Každému sedadlu můžeme přiřadit právě jednoho diváka (totiž uživatele sedadla) a každému diváku právě jedno sedadlo (totiž jeho místo k sezení). Existuje vzájemně jednoznačné zobrazení množiny sedadel na množinu diváků.

U konečných množin se zřejmě vyskytuje právě charakterizovaná souvislost vždy: mají-li A a B stejný počet prvků, existuje vzájemně jednoznačné zobrazení A na B. Můžeme dokonce prvky množin A a B „očíslovat" a přiřadit sobě prvky se stejným číslem. Obráceně, z existence takového zobrazení plyne, že A má právě tolik prvků jako B.

Shrneme-li teď do jedné třídy ty množiny, které mají stejný počet prvků, vznikne tak rozklad všech konečných množin na třídy. Každou třídu můžeme pojmenovat. Třída všech jednoprvkových množin se nazývá „1", třída všech dvouprvkových množin „2", atd. Třídu, která obsahuje jen množinu $\emptyset$, nazveme „0".

Zakladatel teorie množin Georg Cantor[7]) použil ideu vzájemně jednoznačného zobrazení i na nekonečné množiny. To umožnilo zobecnit vztah „A má stejný počet prvků jako B", který byl pro konečné množiny jasný. Do jaké míry to je prospěšné, budeme muset ovšem ještě ukázat.

Definice 1.13. Množiny M_1 a M_2 se nazývají *stejně mohutné* nebo *ekvivalentní*, právě když existuje vzájemně jednoznačné zobrazení M_1 na M_2; píšeme $M_1 \sim M_2$.

---

[7]) Georg Cantor (1845—1918), německý matematik; zabýval se zejména analýzou a topologií; jeho hlavními výsledky jsou aritmetická definice iracionálních čísel a především vytvoření základů teorie množin. Cantor byl také jedním ze zakladatelů německých a mezinárodních matematických kongresů.

Prázdná množina je ekvivalentní pouze sama sobě.

Také pojem stejné mohutnosti množin má vlastnosti uvedené v odstavci 1.2 za D(1.1).

Konečné množiny jsou tedy ekvivalentní, právě když obsahují stejný počet prvků. Jak se D(1.13) projeví u nekonečných množin, vyšetříme nejprve na příkladech.

Přiřaďme každému prvku z N_0 jeho dvojnásobek.

$0 \leftrightarrow 0$	$157 \leftrightarrow 314$
$1 \leftrightarrow 2$	$158 \leftrightarrow 316$
$2 \leftrightarrow 4$	.....
.....	$n \leftrightarrow 2n$
$156 \leftrightarrow 312$	.....

Tak dostaneme ke každému celému nezápornému číslu právě jedno sudé nezáporné číslo a ke každému sudému nezápornému číslu právě jedno celé nezáporné číslo, jak je znázorněno na připojeném schématu; dvojité šipky spojují prvky tímto zobrazením vzájemně přiřazené. N_0 je ekvivalentní množině všech sudých nezáporných čísel. Následující význam této skutečnosti je zpočátku zarážející:

Plně obsazený hotel s nekonečně mnoha jednolůžkovými pokoji, které jsou značeny čísly 1, 2, ..., n, ..., může přijmout ještě další hosty, jestliže se přemístí host z pokoje 1 do pokoje 2, host z pokoje 2 do pokoje 4, host z pokoje 3 do pokoje 6 ... Po tomto přemístění jsou všichni dosavadní hosté ubytováni a všechny pokoje s lichými čísly se uvolnily pro umístění dalších (dokonce nekonečně mnoha) hostů. Zřejmě má N_0 stejnou mohutnost i jako množina Q všech druhých mocnin přirozených čísel, případně i jako množina D všech přirozených čísel dělitelných 10^{10}. Najděte odpovídající vzájemně jednoznačná zobrazení!

N_0 je nekonečná množina. Všechny množiny, které jsou ekvivalentní množině N_0 — mezi něž samozřejmě patří i množina N_0 sama —, se nazývají *spočetně nekonečné množiny*. Toto označení je zvoleno smysluplně, protože je-li M množina ekvivalentní N_0, můžeme každému prvku z M vzájemně jednoznačně přiřadit přirozené číslo. Tímto způsobem budou prvky z M „očíslovány". Předcházející příklady ukazují, že také množina všech sudých čísel a množina všech druhých mocnin přirozených čísel jsou spočetně nekonečné množiny. Cvičení 18 vyžaduje důkaz, že i množina Q^* patří mezi spočetně nekonečné množiny. Tento výsledek udivuje o to víc, že zlomky leží všude „hustě", tj. mezi dvěma libovolně blízkými zlomky z Q^* leží vždy ještě alespoň jeden zlomek.

Jak jsme už zjistili, nemůže se u konečných množin nikdy stát, aby vlastní podmnožina T množiny M byla M ekvivalentní, zatímco u nekonečných množin to je docela dobře možné. Dokonce jsme ukázali, že množina S sudých (nezáporných) čísel, N_0 a Q^* mají stejnou mohutnost, ačkoli platí $S \subset \mathsf{N}_0 \subset \mathsf{Q}^*$ a $S \neq \mathsf{N}_0 \neq \mathsf{Q}^*$.

Zajímavá otázka je, zda existují také *nespočetně nekonečné množiny*, nebo je bohatství nekonečných množin spočetnými množinami už vyčerpáno. Ukážeme, že množina $I = \{x: x \in \mathsf{R} \text{ a } 0 < x < 1\}$ je nejen nekonečná, ale dokonce není ani spočetná. Dokážeme to nepřímo tak, že budeme předpokládat, že I je jen spočetně nekonečná.

Každý prvek z I se dá napsat právě jedním způsobem pomocí svého nekonečného dekadického rozvoje, ve kterém se periodicky neopakuje 9, ve tvaru $x = 0, a_1 a_2 a_3 \ldots$ (např. je $\frac{1}{4} = 0{,}250\ldots$; $\frac{2}{11} = 0{,}\overline{18}\ldots$; $\frac{5}{7} = 0{,}\overline{714285}\ldots$). Kdyby I byla spočetná, existovalo

by alespoň jedno vzájemně jednoznačné zobrazení N_0 na I. Nechť je to následující zobrazení:

$$\begin{aligned}
0 &\leftrightarrow 0,\ a_{01}a_{02}a_{03}a_{04}\ldots &&= x_0,\\
1 &\leftrightarrow 0,\ a_{11}a_{12}a_{13}a_{14}\ldots &&= x_1,\\
2 &\leftrightarrow 0,\ a_{21}a_{22}a_{23}a_{24}\ldots &&= x_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
n &\leftrightarrow 0,\ a_{n1}a_{n2}a_{n3}a_{n4}\ldots &&= x_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Na základě našeho předpokladu musí být v tomto zobrazení zahrnuty všechny prvky $x \in I$. Přesto můžeme určit prvky z I, které se v tomto seznamu nevyskytují. Utvořme $x' = 0, b_1b_2b_3b_4\ldots$ tak, že $b_i = 1$, jestliže $a_{ii} \neq 1$, a $b_i = 2$, jestliže $a_{ii} = 1$. Takto sestrojené číslo x' nemůže být žádné z čísel $x_i \in I$, i když $x' \in I$, neboť $0 < x' < 1$ a $x' \in \mathsf{R}$. Nemůže tedy existovat žádné vzájemně jednoznačné zobrazení N_0 na I; množina I není spočetná. Takováto množina I reálných čísel se nazývá *interval*. Každý interval reálných čísel má stejnou mohutnost jako množina všech reálných čísel. Říkáme, že tyto množiny mají *mohutnost kontinua*. Existují dokonce množiny, které nejsou ani spočetné, ani nepatří k těm, jež mají mohutnost kontinua. Množina všech reálných funkcí definovaných na intervalu I patří mezi ně.

Otevřená ale zůstala ještě úvodní otázka, kdy je jedna množina „menší" než druhá. U konečných množin se pro porovnání velikosti nabízí počet prvků. Pro libovolné množiny můžeme vyslovit následující pravidlo: Množina M_1 má menší mohutnost než množina M_2, právě když M_1 nemá stejnou mohutnost jako M_2, a přitom existuje vlastní podmnožina množiny M_2, která je ekvivalentní M_1.

Co se týče konečných množin, dává tato definice stej-

ný výsledek, jako když porovnáme počet prvků daných množin.

Je zajímavé, že tato definice také dovoluje „odstupňovat" mohutnosti i nekonečných množin. Poznali jsme tři třídy nekonečných množin:

1. Spočetně nekonečné množiny,
2. množiny mohutnosti kontinua,
3. množiny, které nejsou ani spočetné, ani nemají mohutnost kontinua.

Zřejmě každá spočetná množina může být chápána jako vlastní podmnožina nějaké vhodné množiny mohutnosti kontinua, ale ne obráceně. Jsou tedy spočetně nekonečné množiny „menší" než ty, jež mají mohutnost kontinua. Množiny zahrnuté do bodu 3 mají ještě větší mohutnost, než je mohutnost kontinua.

Dodnes ještě zůstává otevřená otázka, zda existuje nekonečná množina, která obsahuje spočetnou množinu jako vlastní podmnožinu, je vlastní podmnožinou množiny mohutnosti kontinua, ale sama nepatří ani k množinám uvedeným v bodě 1, ani k množinám z bodu 2. Mohutnost takové množiny by tedy ležela „mezi" spočetným nekonečnem a kontinuem. Tzv. *hypotéza kontinua* vylučuje existenci takových množin.

1.9 CVIČENÍ

1. Následující množiny zapište ve tvaru $M = \{x : x \in E \text{ a } H(x)\}$.
   a) M_1: množina všech racionálních čísel, jež jsou větší než 2 nebo menší než -2.
   b) M_2: $\{+1; -1\}$.
   c) M_3: množina všech racionálních čísel, jež jsou menší než π a zároveň větší než $\frac{22}{7}$.

2. Tři přímky p_1, p_2, p_3 v rovině jsou popsány následujícími rovnicemi:
$x + 2y = 4$, $x - 2y = 0$, $3x - 2y = 4$.
Určete $p_1 \cap p_2 \cap p_3$ a odůvodněte výsledek.

3. Dokažte, že pro libovolné množiny A, B platí:
a) $A \cup (A \cap B) = A$, b) $(A \setminus B) \cup B = A \cup B$.

4. Dokažte: $A \subset B \subset C \Leftrightarrow A \cup B = B \cap C$.

5. Dokažte: Jsou-li alespoň dvě z množin $A_1, A_2, \ldots, A_n$ disjunktní, pak platí $A_1 \cap A_2 \cap \ldots \cap A_n = \emptyset$. Platí také obrácené tvrzení?

6. Nechť A a B jsou libovolné množiny. Která z následujících tvrzení jsou logicky ekvivalentní?
(1) $A \subset B$, (2) $A \cap B = A$, (3) $A \cup B = B$,
(4) $A \setminus B = \emptyset$.

7. Dokažte následující výrok: Pro libovolnou množinu Z platí (při daných množinách A a B)
$[A \subset Z \text{ a } B \subset Z] \Rightarrow A \cup B \subset Z$.
Tento výrok se dá vyložit takto: Ze všech nadmnožin množin A a B je $A \cup B$ „nejmenší" ve smyslu inkluze. Zformulujte odpovídající výrok pro průnik.

8. Pravdivý, či ne? Vyšetřete následující výroky:
a) Z $A \subset B$ a $B \not\subset C$ plyne $A \not\subset C$.
b) Z $A \not\subset B$ plyne $B \not\subset A$.
c) Z $A \subset B$, $A \neq B$ plyne $B \not\subset A$.
d) Z $A \subset B$ a $A \not\subset C$ plyne $B \not\subset C$.

9. Popište množinu $A \cap (B \cup C)$, jestliže nastane jeden z následujících případů:
a) $A \cap B = \emptyset$, b) $B = C$, c) $A \subset C$, d) $C = \emptyset$, e) $A = \emptyset$.

10. Určete $A \times B \times C$ pro $A = \{0; 2\}$, $B = \{1, 3, 5\}$, $C = \{2; 4\}$.
Z kolika prvků se skládá $A \times B$, jestliže A je r-prvková a B s-prvková množina?

11. Dokažte, že $A \times C = B \times C \Rightarrow A = B$ platí pro libovolné množiny A, B a $C \neq \emptyset$.

12. Která z následujících přiřazení jsou zobrazení?
$F_1 = \{(1, 3), (2, 5), (3, 4), (4, 3), (5,3)\}$ z $M = \{1, 2, 3, 4, 5\}$ do M,
$F_2 = \{(x, y)$: $(x, y) \in \mathbf{N}_0 \times \mathbf{N}_0$ a $y = x$, jestliže x je sudé; $y = x + 1$, jestliže x je liché$\}$ z $\mathbf{N}_0$ do $\mathbf{N}_0$,
$F_3 = \{(x, y)$: $(x, y) \in \mathbf{N}_0 \times \mathbf{N}_0$ a $1 + x < y\}$ z $\mathbf{N}_0$ do $\mathbf{N}_0$,
$F_4 = \{(x, y)$: $(x, y) \in \mathbf{N}_0 \times \mathbf{N}_0$ a $x^2 = y^2\}$ z $\mathbf{N}_0$ na $\mathbf{N}_0$,
$F_5 = \{(x, y)$: $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ a $x^2 = y^2\}$ ze $\mathbf{Z}$ na $\mathbf{Z}$.
Která z těchto přiřazení jsou dokonce vzájemně jednoznačná? Jak se vzájemná jednoznačnost funkce odráží v jejím kartézském grafu, resp. v jejím uzlovém grafu?

13. Pro funkce
$f = \{(x, y)$: $(x, y) \in \mathbf{N}_0 \times \mathbf{N}_0$ a $y = x^2 + 1\}$
a
$g = \{(x, y)$: $(x, y) \in \mathbf{N}_0 \times \mathbf{N}_0$ a $y = 3x + 2\}$
určete $f \circ f$, $g \circ g$, $f \circ g$, $g \circ f$, f^{-1} a g^{-1}.

14. Nechť $M = \{a, b, c, d, e, f, g\}$. Které z následujících podmnožin $\mathcal{P}(M)$ tvoří rozklad M?
a) $\{\{a, b, c\}, \{c\}, \{d, g\}\}$,
b) $\{\{a, e, g\}, \{c, a\}, \{b, e, f\}\}$,
c) $\{\{a, b, e, g\}, \{c\}, \{d, f\}\}$,
d) $\{\{a, b, c, d, e, f, g\}\}$.

15. Uvažujme všechny trojúhelníky v rovině. Je-li T libovolný trojúhelník, třídu $K(T)$ tvoří všechny trojúhelníky podobné T. Zjistěte, zda toto rozdělení je rozklad.

16. Které z následujících množin jsou konečné, které nekonečné?
a) $M_1 = \{x: x \in \mathbf{N}_0$ a $x > 5\}$,
b) $M_2 = \{x: x \in \mathbf{N}_0$ a $x < 100^{100}\}$,
c) $M_3 = \{x: x \in \mathbf{N}_0$ a $x^2 > 100\}$,
d) $M_4 = \{x: x \in \mathbf{N}_0$ a $10^{10} | x\}$,
e) $M_5 = \{x: x \in \mathbf{Q}$ a $0{,}001 < x < 0{,}002\}$,
f) $M_6 = \{x: x \in \mathbf{Z}$ a $x < 1\,000\}$.

17. Ukažte, že množina všech zlomků tvaru $\frac{1}{n}$, kde $n \in \mathbb{N}_0 \setminus \{0\}$ (kmenové zlomky), a také množina všech uspořádaných dvojic přirozených čísel jsou spočetně nekonečné množiny.

18. Dokažte: Množina $\mathbb{Q}^*$ všech zlomků je spočetná.

2. RELACE

VZTAHY JSOU VŠÍM

2.1 POJEM RELACE

Mnohé příklady seznámí čtenáře s pojmem relace a možnostmi jejího popisu

Objekty, jevy a pojmy se často snažíme pochopit tak, že odhalujeme jejich vztahy k jiným objektům, jevům nebo pojmům; např. „Romeo je zamilován do Julie". Tyto vztahy neboli relace mezi objekty často tvoří v našich znalostech právě to podstatné. Tak např. při axiomatické výstavbě geometrie podle Davida Hilberta[8]) se musíme zříci definice základních pojmů jako bod, přímka, rovina; axiómy, z nichž lze odvodit všechny ostatní pojmy a věty euklidovské geometrie, spočívají spíše ve vztazích mezi těmito základními pojmy.

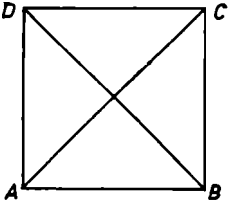
Uveďme teď rozličné příklady:

— Max a Mořic jsou bratři.
— Železo má menší měrnou hustotu než rtuť.
— 4 je dělitel 256, tj. $4|256$.
— Erfurt je od Gothy vzdálen nejvýše 100 km.
— Množina prvočísel je obsažena v množině celých čísel.
— 6 je nesoudělné se 49, tj. $D(6, 49) = 1$.

---

[8]) David Hilbert (1862—1943), německý matematik; přispěl k mnoha oblastem matematiky, např. k teorii čísel, teorii invariantů, teorii algebraických variet, teorii integrálních rovnic, variačnímu počtu, k základům matematiky, ale i k teoretické fyzice. Přesná axiomatická výstavba geometrie je obsahem jeho práce „Die Grundlagen der Geometrie", která vyšla v r. 1899 v nakladatelství Teubner-Verlag.
Rovněž významně přispěl k dalšímu rozvoji matematiky svými slavnými 23 problémy. (Pozn. překl.)

— Z „$ABCD$ je čtverec“ plyne „úhlopříčky $ABCD$ se navzájem půlí“; tj. $ABCD$ čtverec $\Rightarrow$ úhlopříčky $ABCD$ se navzájem půlí (obr. 10).



Obr. 10

— Xantipa je sprízněna se Sokratem.
— 36 je násobek 9.
— „Škola“ stojí v abecedě před „šupinou“.
— 18 má právě tolik dělitelů jako 50.
— 623 dává při dělení třemi stejný zbytek jako 263, tj. $623 \equiv 263 \pmod 3$.
— 623 má stejný ciferný součet jako 263.
— 4 je menší než 256, tj. $4 < 256$.
— Gotthelf, Erich a Herbert Abrahám mají stejné příjmení.
— Zlomek $\frac{2}{3}$ dává stejný podíl jako $\frac{18}{27}$, tj. $\frac{2}{3} = \frac{18}{27}$.
— Přímka AB na obr. 10 je rovnoběžná s přímkou CD, tj. $AB \parallel CD$.
— Přímka AC na obr. 10 je kolmá k přímce BD, tj. $AC \perp BD$.
— 2 je prvkem množiny prvočísel.

Pokusme se z těchto příkladů odvodit obecný pojem relace. Nejprve si všimněme, že obecně jsou ve vzájem

ném vztahu (např. je dělitel, má menší měrnou hustotu. je vzdálen nejvýše 100 km, stojí v abecedě před, je obsažen v, z ... plyne) vždy dva prvky množiny M (např. množiny přirozených čísel, množiny chemických prvků, množiny měst jedné země, množiny slov českého jazyka, množiny podmnožin reálných čísel, množiny výroků). Říkáme, že prvky množiny M jsou v relaci; tak např. prvky 4 a 256 jsou v relaci „je dělitel". Obecně zřejmě záleží na pořadí prvků; prvky 256 a 4 nejsou v relaci „je dělitel". Dají se tedy prvky $x, y \in M$ v nějaké dané relaci R chápat jako uspořádané dvojice (x, y) (srov. odstavec 1.5) a relaci R v M můžeme charakterizovat jako tu podmnožinu kartézského součinu $M \times M$, jež obsahuje právě všechny uspořádané dvojice (x, y) takové, že x je v relaci R s y. Je-li x s y v relaci R, píšeme $(x, y) \in R$, nebo stručněji xRy. Obráceně určuje každá podmnožina $T \subset M \times M$ relaci R v M předpisem: xRy, právě když $(x, y) \in T$.

Definice 2.1. *Relací R v množině M* rozumíme libovolnou podmnožinu kartézského součinu $M \times M$.

Příklady. Je-li R relace „menší než" v množině M celých čísel od 0 do 5, můžeme R vyjádřit jako podmnožinu $M \times M$:

$R = \{(0, 1), (0, 2), (0, 3), (0, 4), (0, 5), (1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$.

Relace $R = \{(1, 2), (1, 3), (1, 4), (2, 4)\}$ v množině $M = \{1, 2, 3, 4\}$ se dá popsat také takto: xRy, právě když $x < y$ a $x|y$. (Srov. popis množiny výčtem jejích prvků, příp. udáním charakteristické vlastnosti!)

Každá podmnožina R součinu $M \times M$ definuje relaci v M, tedy také množiny $R_0 = \emptyset$, $R_t = M \times M$ a $R_i = \{(x, x): x \in M\}$. Relace $R_0 = \emptyset$ se nazývá *nulová relace v M*; v této relaci nejsou žádné dva prvky. $R_t =$

$= M \times M$ se nazývá *totální relace v* M. A konečně relaci R_i říkáme *identita v* M (nebo také *diagonála*), neboť xR_iy platí, právě když $x = y$.

Pohled zpět na odstavec 1.7 ukazuje, že relaci v M můžeme také chápat jako přiřazení z M do M; v tomto smyslu mluvíme pak také o definičním oboru a oboru hodnot relace R ($\mathscr{D}(R)$, resp. $\mathscr{H}(R)$).

Zrovna tak je možné skládat dvě relace jako přiřazení.

Mnohý čtenář si už jistě všiml, že definice relace D(2.1) se nedá použít na příklad „2 je prvek množiny prvočísel", ačkoli bychom přece jen asi chtěli „je prvek" za relaci považovat. Tato relace ale dává do vztahu prvky množiny A (zde množiny N_0 celých nezáporných čísel) s prvky jiné množiny B (zde potenční množiny množiny N_0, ze které je vzata jako jeden z jejích prvků množina prvočísel). Proto abychom zahrnuli i takové případy, rozšíříme definici relace následovně:

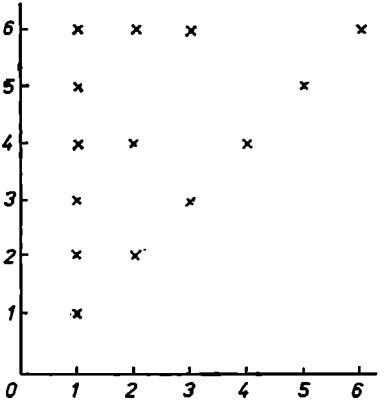
Definice 2.2. *Relace* R mezi množinami A a B je podmnožina kartézského součinu $A \times B$.

Pro takové relace můžeme jako příklad uvést ještě relaci „leží na" mezi množinou A všech bodů v rovině a množinou B všech přímek této roviny.

V následujícím ale přece jen zůstaneme u relací v množině M; takové relace můžeme popsat různými způsoby. Je-li množina M konečná, může být relace v M (v principu) dána výčtem uspořádaných dvojic $(x, y) \in M \times M$ patřících do R, např. relace $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6)\}$ v množině $M = \{1, 2, 3, 4, 5, 6\}$.

Uvědomme si však, že relace R v M je množina, totiž podmnožina $M \times M$, takže ji můžeme jako každou množinu také popsat nějakou charakteristickou vlast-

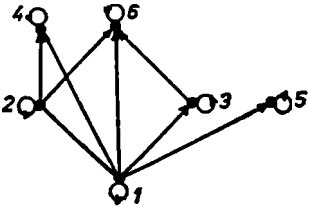
ností, která je splněna právě pro ty uspořádané dvojice ze základní množiny $M \times M$, jež patří do R. Předchozí relace R může být takto charakterizována jako $R = \{(x, y): x, y \in M \text{ a } x|y\}$, kde $M = \{1, 2, 3, 4, 5, 6\}$.



Obr. 11

Protože každou (binární) relaci R v M můžeme také chápat jako přiřazení, můžeme pro znázornění R stejně jako u přiřazení nakreslit graf relace, jak je vidět na obr. 11 opět pro relaci „je dělitel" v množině $M = \{1, 2, 3, 4, 5, 6\}$. Stejně dospějeme i k uzlovému grafu relace; je ovšem běžné pro relace v M nekreslit oba exempláře oblasti roviny odpovídající množině M, nýbrž jen jeden, jak vidíme na obr. 12 opět pro shora uvedenou relaci. Pro každé x takové, že xRx, se pak musí namalovat šipka z P_x do P_x, což naznačíme malou „kruhovou" šipkou okolo P_x. Zřejmě závisí na relaci a na účelu, jakému znázornění dáme přednost; v našem příkladu

uzlový graf jistě dává názornější představu o uvedené relaci. Naopak dříve zavedené relace R_0 (nulová relace), R_t (totální relace) a R_i (identita na M) mají zvlášť přehledný kartézský graf. Jak vypadají? Např. graf relace R_i objasňuje, proč se této relaci také říká „diagonála M".



Obr. 12

V našich úvahách jsme relací vždy rozuměli množinu uspořádaných dvojic (x, y), kde $x, y \in M$ v případě relace v M, resp. $x \in A$, $y \in B$ v případě relace mezi A a B. Chceme-li ale např. relaci „býti mezi" (reálné číslo x leží mezi reálnými čísly y a z) podřídit tomuto množinově teoretickému nazírání, musíme — vzhledem ke třem proměnným x, y, z — přejít k uspořádaným trojicím (x, y, z), tedy k podmnožinám kartézského součinu $M \times M \times M$. Takovým relacím říkáme *ternární relace*. Obecně rozumíme k-nární relací v M podmnožinu kartézského součinu $M \times M \times \ldots \times M$. V této kapitole jsme se tedy zabývali jen binárními relacemi. Ani zde uvedený k-násobný kartézský součin nemusí mít samozřejmě všechny činitele vesměs rovné M. Bez tohoto omezení pak dalším zobecněním dojdeme k pojmu k-nární relace v $M_1 \times M_2 \times \ldots \times M_k$. Platí-li $(x_1, x_2, \ldots, x_k) \in R$, říkáme, že k-tice $(x_1, x_2, \ldots, x_k)$ je v k-nární relaci R.

2.2 VLASTNOSTI RELACÍ

Tato kapitola se zabývá vlastnostmi relací, jako je např. reflexivita, symetrie, tranzitivita; položíme si otázku, zda z některých těchto vlastností neplynou ostatní

Skutečnost, že Max je bratr Mořice, jsme vyjádřili jako „Max a Mořic jsou bratři". V této formulaci se už ale skrývá další informace o relaci „je bratr". To je nejlépe patrné, pokusíme-li se přejít od výroku „4 je dělitel 256" k formulaci „4 a 256 jsou dělitelé". Poslední výrok je podle toho, jaký máme vztah k jazyku, nesmyslný anebo polopravdivý. Pokus o přeformulování nemohl být úspěšný proto, že v uvedeném příkladu záleží na pořadí prvků 4 a 256, zatímco v prvním příkladu pořadí nehraje žádnou roli: je-li Max bratr Mořice, je také Mořic bratr Maxe. Relace s touto vlastností se nazývají *symetrické*. Přitom mlčky předpokládáme, že M je neprázdná.

Definice 2.3. Relace R v M se nazývá *symetrická*, právě když pro všechna $x, y \in M$, pro něž platí xRy, je také yRx; jinak řečeno: xRy a yRx platí vždy současně.

Příklady. (1) Relace „je rovnoběžný s" v množině přímek nějaké roviny je symetrická, neboť je-li $g \parallel h$, je také $h \parallel g$. Můžeme tedy také říci, že obě přímky g a h jsou navzájem rovnoběžné.

(2) Relace „dává při dělení třemi stejný zbytek" je symetrická, neboť $a \equiv b \pmod 3$ znamená $a = b + 3c$, c celé, odkud ihned plyne $b = a + 3(-c)$, tedy $b \equiv a \pmod 3$, neboť $(-c)$ je stejně jako c celé číslo.

(3) Relace „je zamilován(a) do" uvažovaná v dostatečně velké množině lidí je zjevně nesymetrická, protože

xRy ne vždy znamená yRx; právě to bývá příčinou nešťastné lásky.

(4) Relace „z ... plyne“ definovaná v množině výroků, v řeči jinak formulovaná jako „jestliže ..., pak“, kterou budeme v dalším nazývat vždy implikace, není symetrická, jak poznáme z následujícího protipříkladu: Výrok „$ABCD$ je čtverec $\Rightarrow$ úhlopříčky $ABCD$ se navzájem půlí“ je správný. Naproti tomu jeho obrácení „úhlopříčky $ABCD$ se půlí $\Rightarrow$ $ABCD$ je čtverec“ správné není, neboť i v obdélníku se úhlopříčky půlí.

Tento příklad obrací naši pozornost ještě jednou na ono místo v definici symetrie, na kterém se říká, že spolu s xRy má zároveň platit yRx. Je-li tento požadavek jen jednou porušen, není R symetrická. Tato poznámka je důležitá v souvislosti s implikací, protože bychom přirozeně mohli najít dostatečně mnoho příkladů výroků zaměnitelných vzhledem k implikaci, např. „celé číslo c je dělitelné třemi $\Rightarrow$ ciferný součet čísla c je dělitelný třemi“, přičemž je správná i obrácená implikace. V takových případech místo „$\Rightarrow$“ píšeme oboustrannou šipku „$\Leftrightarrow$“, kterou čteme jako „je logicky ekvivalentní“ nebo „tehdy a jen tehdy, když“, anebo „právě když“. *Logická ekvivalence* je tudíž symetrická relace a mohli bychom — vrátíme-li se k předchozímu příkladu —, říci: „Dělitelnost čísla třemi je ekvivalentní dělitelnosti jeho ciferného součtu třemi“. Zřejmě je pro použití matematické věty velmi důležité vědět, zda má logickou strukturu implikace nebo ekvivalence.

(5) Zatímco implikace se ukázala jako nesymetrická relace, tj. jako taková, v níž existují jak dvojice (x, y), pro něž zároveň platí xRy i yRx, tak i dvojice, pro něž je sice splněno xRy, ale ne yRx, poskytuje relace „menší než“ příklad relace tzv. *asymetrické*, v níž xRy a yRx není nikdy splněno současně. Přejdeme-li od relace „$<$“ k relaci „$\leqq$“, pak existují dvojice prvků (x, y), pro

něž platí jak $x \leqq y$, tak i $y \leqq x$, totiž právě ty dvojice, kde $x = y$. Relace R s vlastností, že z xRy a yRx plyne vždy $x = y$, se nazývají *antisymetrické*, taková je např. relace „je dělitel" v množině celých kladných čísel. Rozmyslete si, jak se symetrická relace pozná podle svého grafu, resp. uzlového grafu.

V našem úvodním příkladu se také vyskytla formulace „Gotthelf, Erich a Herbert Abraham mají stejné příjmení", která — to už teď víme —, může být správná, jen když je relace „má stejné příjmení jako" symetrická. Tak tomu vskutku je. Ale to, že tu spolu stojí víc než dva prvky se společným příznakem, v tom hraje roli ještě další vlastnost relace. Uvažujme rovněž symetrickou relaci „je vzdálen nejvýše 100 km od". Ačkoli jsou teď oba výroky „Gotha je vzdálena nejvýše 100 km od Erfurtu" a „Erfurt je vzdálen nejvýše 100 km od Merseburgu" správné, nemůžeme říci, že „Erfurt, Gotha a Merseburg jsou od sebe navzájem vzdáleny nejvýše 100 km", neboť vzdálenost Gotha — Merseburg je větší než 100 km. Uvedená relace R se tedy nedá „přenášet", nemá vlastnost, která se nazývá *tranzitivita:* Jestliže xRy a yRz, pak také xRz.

Definice 2.4. Relace R v M se nazývá *tranzitivní*, právě když pro všechna $x, y, z \in M$, pro něž platí xRy a yRz, je také xRz; jinak řečeno: Z xRy a yRz vždy plyne xRz.

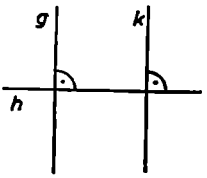
Příklady. (1) Relace „je menší než" v Z je tranzitivní, neboť z $x < y$ a $y < z$ plyne ihned $x < z$. To je zároveň příkladem relace, která je asymetrická, ale tranzitivní.

(2) Relace „je dělitel" v $\mathbb{N}_0 \setminus \{0\}$ je tranzitivní. Platí-li totiž $a \mid b$ a $b \mid c$, takže podle definice relace dělitelnosti existují přirozená čísla s a t taková, že $b = sa$ a $c = tb$, odkud plyne $c = t(sa) = (ts)\,a$. Protože ts je celé kladné číslo, dostáváme odtud $a \mid c$. Tato relace tedy poskytuje příklad antisymetrické a tranzitivní relace.

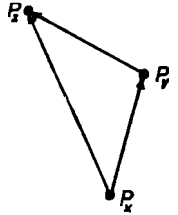
(3) Důležitým příkladem nesymetrické, ale tranzitivní relace je implikace. Vždyť na tranzitivitě této relace podstatně závisí matematický úsudek.

(4) Symetrická relace „dává při dělení třemi stejný zbytek" je také tranzitivní: Z $a \equiv b \pmod 3$ a $b \equiv c \pmod 3$, tj. $a = b + 3g$ a $b = c + 3h$ pro g, h celá, plyne $a = (c + 3h) + 3g = c + 3(h + g)$, tedy $a \equiv c \pmod 3$, neboť spolu s g a h je i $h + g$ celé číslo.

(5) Relace „je kolmý na" v množině přímek jedné roviny je symetrická, jak ihned zjistíme, ale není tranzitivní (obr. 13).



Obr. 13



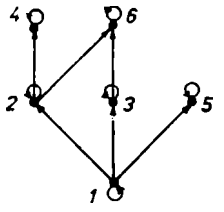
Obr. 14

(6) Příklad relace, jež není ani symetrická, ani tranzitivní, najdeme třeba v relaci „je první derivací" v množině libovolněkrát derivovatelných funkcí nebo v relaci „je strýc", o relaci „je zamilován do" ani nemluvě.

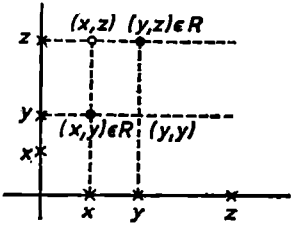
Velmi zřetelně se tranzitivita odráží v uzlovém grafu relace: S libovolnými dvěma na sebe „navazujícími" šipkami z P_x do P_y a z P_y do P_z patří do grafu také „přemosťující" šipka z P_x do P_z (obr. 14). Můžeme se tedy dohodnout na zjednodušení uzlového grafu tranzitivní relace, při němž odstraníme šipku z P_x do P_z, jestliže graf už obsahuje dvě šipky (z P_x do P_y a z P_y do P_z), jejichž přemostěním je šipka z P_x do P_z. Uzlový graf tranzitivní relace „je dělitel" v $M = \{1, 2, 3, 4, 5, 6\}$

na obr. 12 se podle této úmluvy zjednoduší na graf znázorněný na obr. 15.

Obr. 16 ilustruje, jak lze tranzitivitu poznat na kartézském grafu relace R: Leží-li jeden ze čtyř vrcholů obdélníku se stranami rovnoběžnými s osami na diagonále a oba jeho sousední vrcholy jsou body grafu relace R, pak do grafu R musí vždy patřit i čtvrtý vrchol. Podle obr. 16 pro to snadno najdete odůvodnění.



Obr. 15



Obr. 16

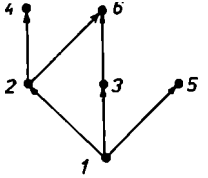
V matematice se často užívají relace k tomu, abychom rozdělili prvky nějaké množiny M do tříd rovnocenných prvků (srov. odstavec 2.3). Tak např. v euklidovské geometrii rozlišujeme shodné útvary, ale díváme se na ně jako na „rovnocenné"; právě tak jako na zlomky, které se dají na sebe převést krácením nebo rozšířením. Přirozeně, taková relace rovnocennosti v sobě zahrnuje i obvyklou rovnost, tj. každý prvek množiny M je sám sobě rovnocenný. Relace R v M, která má být relací rovnocennosti, proto musí mít vlastnost xRx pro všechna $x \in M$. Tato vlastnost se nazývá *reflexivita*.

Definice 2.5. Relace R v M se nazývá *reflexivní*, právě když pro všechna $x \in M$ platí xRx. Není-li naopak xRx splněno pro žádné $x \in M$, nazývá se R *ireflexivní*.

Okamžitě zjistíme, že relace „je dělitel", „je vzdálen nejvýše 100 km od", „má právě tolik dělitelů jako", „dává při dělení třemi stejný zbytek jako", „dávají stejný podíl", „je rovnoběžný s" stejně jako implikace jsou reflexívní. Ireflexívní jsou naproti tomu relace „je lehčí než", „stojí v abecedě před", „je menší než", „je kolmý k". Relace $R = \{(x, y)$: xy je liché$\}$ v množině celých čísel není reflexívní, neboť xRx zřejmě platí jen pro lichá x. Tento příklad mimo jiné ukazuje, že je třeba rozlišovat „ireflexívní" a „nereflexívní". Podobně relace „je zamilován do" není reflexívní, ale ani ireflexívní, neboť vztah xRx sice obecně neplatí, ale je správný pro x = Narcis[9]).

Do grafu reflexívní relace patří všechny body (x, x) diagonály, a obráceně, graf s touto vlastností je grafem reflexívní relace.

U uzlového grafu jsme se už dohodli, že platnost vztahu xRx budeme vyjadřovat malou kruhovou šipkou okolo bodu P_x přiřazeného x. Je-li R reflexívní, pak každému bodu z M přísluší kruhová šipka, a tak můžeme graf dále zjednodušit smluveným odstraněním těchto kruhových šipek. Pro relaci „je dělitel" v $M = \{1, 2, 3, 4, 5, 6\}$ tak dospějeme od grafu na obr. 15 ke grafu na obr. 17.



Obr. 17

[9]) Narcis: v řecké báji krásný jinoch, který za to, že pohrdl láskou nymfy Échy, byl potrestán tím, že se zamiloval do svého vlastního obrazu.

Budeme nyní zkoumat, zda dosud uvažované vlastnosti relací jsou navzájem nezávislé, anebo z některé z těchto vlastností nutně plyne jiná.

Nejdříve ukažme, že tři „základní vlastnosti", reflexivita, symetrie a tranzitivita, jsou navzájem nezávislé, neboť z libovolných dvou těchto vlastností nemusí nutně plynout ta třetí. Mezi našimi příklady snadno najdete relace, jež jsou

— reflexívní a symetrické, ale ne tranzitivní;
— reflexívní a tranzitivní, ale ne symetrické;
— symetrické a tranzitivní, ale ne reflexívní.

Tady se také vyplatí důkladněji si rozmyslet logickou strukturu důkazu: Abychom dokázali tvrzení A (nezávislost tří základních vlastností), ukážeme, že není správný výrok „ne A". Tento nepřímý důkaz bude proveden, jestliže ke každému možnému případu závislosti oněch tří vlastností udáme protipříklad.

Naproti tomu jiné vlastnosti relace mohou být navzájem zcela závislé, jak ukazuje následující věta.

Věta 2.1. *Pro libovolnou relaci R v M platí:*
a) R je *asymetrická* $\Rightarrow$ *R je ireflexívní*;
b) *R je ireflexívní a tranzitivní* $\Rightarrow$ *R je asymetrická.*

Důkaz. (a) Protože R je asymetrická, neplatí xRy a yRx zároveň, neplatí tedy zároveň ani pro $x = y$, to ale znamená, že xRx není splněno pro žádné $x \in M$. Je tedy R ireflexívní.

(b) K důkazu asymetrie R je potřeba ukázat, že vztahy xRy a yRx nenastanou současně. Důkaz provedeme nepřímo tak, že z předpokladu existence dvojice (x_0, y_0), pro niž je zároveň x_0Ry_0 i y_0Rx_0, dojdeme ke sporu s jedním z předpokladů tvrzení. Z platnosti vztahů x_0Ry_0 a y_0Rx_0 však plyne díky předpokládané tranzitivitě x_0Rx_0, a to je spor s předpokladem ireflexivity, podle

níž nemůže být xRx pro žádný prvek z M. Je tedy náš předpoklad nesprávný, a platí tudíž jeho opak, tj. tvrzení věty, c. b. d.

V matematice se často využívá věty o rovnosti třetímu: „Jsou-li dvě velikosti rovny třetí, tak jsou rovny také navzájem.“ Ptáme se: Na základě které vlastnosti relace R můžeme tento úsudek použít i na R?

Věta 2.2. *Pro symetrickou a tranzitivní relaci R v M platí: Z xRz a yRz vždy plyne xRy (rovnost třetímu).*

Důkaz. Nechť x, y, z jsou libovolné prvky M takové, že xRz a yRz. Díky symetrii R můžeme od (xRz a yRz) přejít k výroku (xRz a zRy), odkud díky tranzitivitě R hned plyne xRy, c. b. d.

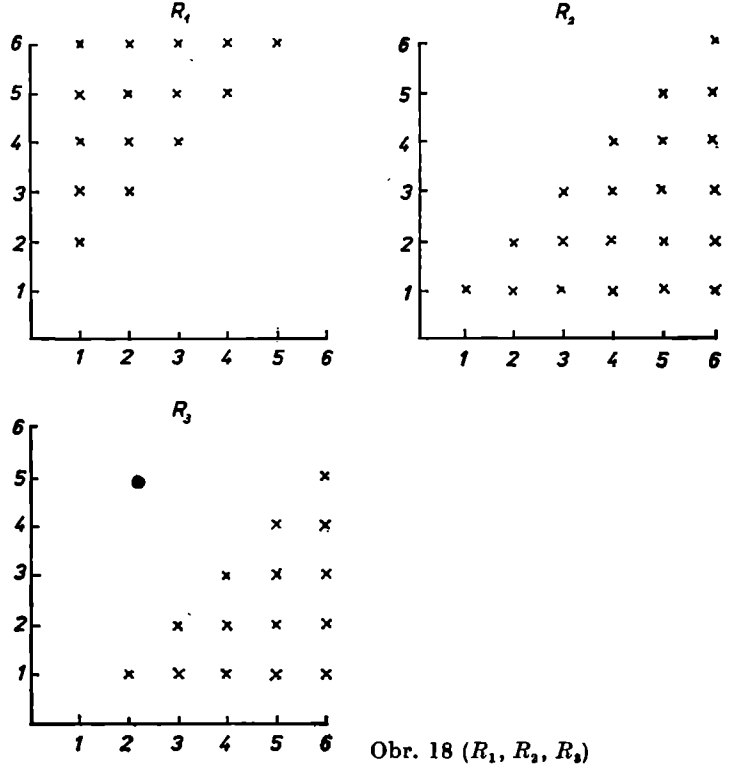
Obráceně plyne také symetrie a tranzitivita z rovnosti třetímu, ovšem jen pro reflexívní relace. To nahlédneme takto: Předpokládejme, že (xRz a yRz) $\Rightarrow xRy$. Pro $z = x$ odtud dostaneme (xRx a yRx) $\Rightarrow xRy$. A protože díky předpokládané reflexivitě platí xRx pro všechna $x \in M$, uvedená implikace se zjednoduší na $yRx \Rightarrow xRy$, to ale znamená, že R je symetrická. R je rovněž tranzitivní, neboť z (xRy a yRz) plyne díky shora dokázané symetrii (xRy a zRy), takže na základě předpokládané rovnosti třetímu odtud plyne xRz.

Nakonec se ještě vyplatí podívat se trochu na zřejmou příbuznost relací „je menší než“, „není menší než“, „je větší než“, případně relací „$=$“ a „$\neq$“ nebo relací „je dělitel“ a „je násobek“.

Znázorněme relace

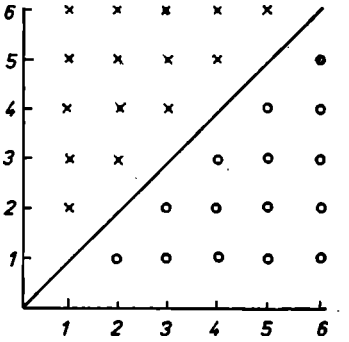
$R_1 = \{(x, y)$: x je menší než $y\} = \{(x, y)$: $x < y\}$,
$R_2 = \{(x, y)$: x není menší než $y\} = \{(x, y)$: $x \geqq y\}$,
$R_3 = \{(x, y)$: x je větší než $y\} = \{(x, y)$: $x > y\}$

v množině $M = \{1, 2, 3, 4, 5, 6\}$ kartézským grafem (obr. 18). Zjistíme, že z 36 prvků $M \times M$ patří do R_2 právě ty, které nepatří do R_1, a naopak do R_1 patří právě ty, jež nepatří do R_2, což lze zjistit už ze slovního vyjádření relací. Z hlediska teorie množin je tedy R_2 doplňkem množiny R_1 vzhledem k základní množině $M \times M$ (srov. kapitolu 1). Analogicky k tomuto ozna-



Obr. 18 (R_1, R_2, R_3)

čení se relace $R' = \{(x, y)\colon (x, y) \in M \times M \text{ a } (x, y) \notin R\}$ příslušná k relaci R (v M) nazývá *doplňková relace k R*. Z této definice hned plyne, že doplňková relace k relaci doplňkové k R je zase relace R; píšeme $(R')' = R$. Zobrazení, které každé relaci přiřazuje její doplňkovou relaci, je tudíž involutorní, takže relace R a R' můžeme nazývat *navzájem doplňkové*.



Obr. 19

Na obr. 19 jsou sestrojeny grafy relací R_1 a R_3 ve stejné soustavě souřadnic; body patřící do R_1 jsou označeny křížky, body patřící do R_3 kroužky. Je vidět, že grafy R_1 a R_3 leží souměrně podle diagonály: bod (x, y) patří do grafu R_3, právě když bod (y, x) patří do grafu R_1. Podíváme-li se na relaci v M jako na přiřazení z M do M, je R_3 právě inverzní přiřazení k R_1, a naopak. Můžeme proto zavést pojem relace R^{-1} inverzní k relaci R v M prostřednictvím definice:

$$R^{-1} = \{(x, y)\colon (x, y) \in M \times M \text{ a } (y, x) \in R\}.$$

Stejně jako pro přiřazení, platí také zde přirozeně

$(R^{-1})^{-1} = R$; můžeme tudíž R a R^{-1} označovat jako *navzájem inverzní*. Další příklad dvou navzájem inverzních relací najdeme v relaci „je dělitel" a „je násobek", neboť $x \mid y$ znamená $y = cx$, c celé, to ale znamená, že y je násobek x, a obráceně.

Zodpovězení zajímavé otázky, jaké relace mají vlastnost $R = R^{-1}$, přenecháváme čtenáři; dostane se tak námi už studovaná třída relací, které se tudíž dají charakterizovat i rovností $R = R^{-1}$.

Na závěr ještě uvážíme, které vlastnosti relace R se přenášejí na R^{-1}, případně R'.

Věta 2.3. (1) *Reflexivita, ireflexivita, symetrie, asymetrie, antisymetrie a tranzitivita se přenášejí z R na R^{-1}.*
(2) *Při přechodu od R k R' se přenáší symetrie, zatímco reflexivita přechází v ireflexivitu, a naopak.*

Důkaz. Tvrzení spojuje dohromady devět jednotlivých výroků (které?) Všechny důkazy probíhají podle stejného schématu, takže se zde spokojíme s jedním vzorem. Ostatní si rozmyslete jako cvičení.

Nechť R je tranzitivní, ukážeme tranzitivitu R^{-1}. Je-li $(x, y), (y, z) \in R^{-1}$, je $(y, x), (z, y) \in R$. Protože R je tranzitivní, plyne odtud $(z, x) \in R$, takže $(x, z) \in R^{-1}$, c. b. d.

Přenesení symetrie z R na R' ukážeme nepřímo. Kdyby R' nebyla symetrická, existovala by alespoň jedna dvojice (x_0, y_0) taková, že $(x_0, y_0) \in R'$, ale $(y_0, x_0) \notin R'$. Z definice doplňkové relace plyne, že pak $(y_0, x_0) \in R$, ale díky symetrii R odtud dostáváme $(x_0, y_0) \in R$, což je ve sporu s předpokladem, že $(x_0, y_0) \in R'$. Je tedy R' spolu s R také symetrická, c. b. d.

2.3 RELACE EKVIVALENCE

Čtenář se seznámí s jedním ze základních pojmů matematiky, s pojmem ekvivalence v M a s jeho souvislostí s rozklady M

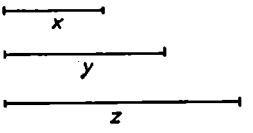
„Rovný rovného si hledá", říkává nesouhlasně teta Herma, když chuligán Mike odvádí svého kumpána Freda ke každovečerním toulkám. Přitom Mike a Fred byli všechno možné, jen ne stejní; Mike byl malý a rezavý, Fred zas kudrnatý černovlasý atlet, a o dva roky mladší než Mike. Je přirozeně jasné, že teta mínila své úsloví docela jinak. Použije-li někdo toto úsloví, užívá slovo „rovný" ne ve smyslu absolutní identity, podle níž je věc rovna jen sama sobě, nýbrž v rozšířeném smyslu „rovnocennosti" neboli „rovnosti vzhledem k jednomu či více daným příznakům". Dvě věci, které se vzhledem k nějakému příznaku rovnají, i když jinak mohou být zcela rozdílné, nazýváme často ekvivalentní vzhledem k tomuto příznaku.

Při rozdávání učebnic na nový školní rok se na všechny žáky hledí jako na „rovné", patří-li do téhož ročníku, neboť dostávají stejné knihy. V tomto smyslu existuje jen 10, resp. 12 různých skupin žáků.

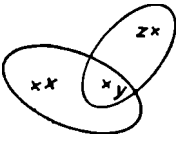
Pro upevnění pojmu „barva" dostávají děti v mateřské škole úlohu rozdělit různé předměty podle barev. Přitom se musí naučit nebrat zřetel na tvar, funkci a materiál předmětu a jako klasifikačního příznaku používat jen jeho barvu. Tak bude množina tříděných předmětů rozložena do tříd objektů stejné barvy (srov. odstavec 1.7). Jiný klasifikační princip může přirozeně vést ke zcela jinému rozkladu téže základní množiny. Máme-li např. dřevěné tyčky různých barev, délek a tvarů průřezu, je zpočátku pro děti obtížné přejít od jednoho rozkladu k jinému. Aby mohlo takový rozklad

provést, musí mít dítě schopnost zjistit u každých dvou objektů, zda jsou v relaci „rovný vzhledem k uvedenému příznaku“, nebo ne.

Zřejmě existuje užší souvislost mezi rozkladem množiny M a „klasifikačním principem“, který takový rozklad vyvolává. Příklad relace „je nejvýše o 1 cm delší než“ v množině dřevěných tyček ale ukazuje, že ne každou relaci můžeme použít jako klasifikační princip.



Obr. 20



Obr. 21

Obr. 20 ukazuje, že vzhledem k této relaci jak x a y, tak i y a z leží ve stejné třídě, ne ale x a z; tj. třídy K_x a K_z nejsou ani identické (neboť $x \in K_x$, ale $x \notin K_z$), ani disjunktní (neboť $y \in K_x \cap K_z$). To nás přivádí k tomu, abychom se zabývali otázkou položenou už v závěru odstavce 1.7, totiž jaké vlastnosti musí mít relace R v M, aby vznikl rozklad M. Uvažujme proto nějaký rozklad $\mathfrak{Z}$ množiny M a relaci R v M takovou, že xRy, právě když x leží v téže třídě rozkladu jako y. Zřejmě je R reflexívní, neboť především leží každé $x \in M$ alespoň v jedné třídě rozkladu, a pak — triviálně — v téže třídě jako x. Leží-li x v téže třídě jako y, leží také y v téže třídě jako x, tj. spolu s xRy platí i yRx. Je tedy R symetrická. Konečně je R tranzitivní, neboť leží-li x v téže třídě jako y a y v téže třídě jako z, musí také x a z ležet v této třídě. Přitom jsme podstatně použili disjunktnost tříd; jinak by také mohl nastat případ zachycený na obr. 21, který nedovoluje závěr „x leží v téže třídě jako z“.

Naše úvahy ukázaly, že každý rozklad M vede k definici reflexívní, symetrické a tranzitivní relace R v M. Než ukážeme, že také obráceně každá taková relace v M dává rozklad M, relaci s těmito vlastnostmi pojmenujeme.

Definice 2.6. Relace R v množině M se nazývá relace *ekvivalence v* M, právě když je reflexívní, symetrická a tranzitivní.

Nyní se budeme věnovat hlavní větě o relacích ekvivalence, která popisuje souvislost mezi rozklady množiny M a v M definovanými relacemi ekvivalence.

Věta 2.4. (1) *Každá relace ekvivalence R v M dává rozklad M.*
(2) *Každý rozklad $\mathfrak{Z}$ množiny M můžeme dostat z relace ekvivalence v M.*

Než přistoupíme k důkazu této věty, chtěli bychom zjistit spojitost mezi relací ekvivalence a rozkladem. Nechť $M = \mathsf{N}$ je množina přirozených čísel a relace R v N nechť je definována takto: xRy, právě když se x a y liší nejvýše poslední číslicí. R je relace ekvivalence, jak hned zjistíme ověřením všech tří vlastností — reflexivity, symetrie a tranzitivity. Abychom viděli, na jaké třídy vzhledem k R se N rozloží, určíme ke každému $x \in \mathsf{N}$ množinu K_x všech přirozených čísel, která jsou s x v relaci R. Vezmeme-li např. $x = 561$, sestává K_{561} ze všech těch přirozených čísel, která se liší od 561 nejvýše poslední číslicí, tj. $K_{561} = \{560, 561, 562, \ldots, 569\}$. Na tomto příkladě hned zjistíme, že relace ekvivalence R rozděluje N na „desítky". Je také zřejmé, že je to rozklad N ve smyslu odstavce 1.7, neboť díky $x \in K_x$ patří každé přirozené číslo x do nějaké třídy a žádná třída není prázdná. Musíme tedy ještě

uvážit, že dvě třídy K_x a K_y mohou být jen totožné nebo disjunktní. První případ pak nastane určitě tehdy, když se x a y liší pouze poslední číslicí; např. je zřejmé $K_{561} = K_{568}$. Předpokládejme, že K_x a K_y nejsou disjunktní, mají tedy alespoň jeden prvek z společný. Pak by se lišilo jak z od x, tak i z od y nejvýše na posledním místě, tj. xRz a yRz. Protože R je relace ekvivalence, plyne odtud xRy, tj. také x a y se liší nejvýše na posledním místě. Je tedy $K_x = K_y$, což je zde díky jednoduchosti uvažované relace vidět hned, obecně to ale musíme dokazovat. Ukázali jsme tak, že nedisjunktní třídy jsou totožné, musí tedy být různé třídy disjunktní.

Relace ekvivalence R nás tedy vskutku přivedla k rozkladu N na třídy. Vyjdeme-li naopak z rozkladu N, třeba z rozkladu na „desítky", a definujeme-li relaci R v N tak, že xRy, právě když x a y leží v téže třídě rozkladu (tj. v téže „desítce"), zjistíme, že R je relace ekvivalence. Nyní se můžeme opět nechat přivést k rozkladu N, jak jsme vysvětlili předtím, a v našem příkladu je jisté, že zas dostaneme výchozí rozklad N. Po těchto přípravách nebude nyní těžké sledovat důkaz V(2.4).

Důkaz (1). Ke každému $x \in M$ určíme množinu K_x všech prvků $y \in M$, které jsou s x v relaci R, přesněji $K_x = \{y: y \in M \text{ a } xRy\}$, a nazveme ji — poněkud předčasně — třída určená x. Přirozeně se lze domnívat, že souhrn všech těchto tříd dává rozklad M. Na důkaz ověřme tři vlastnosti rozkladu (srov. odstavec 1.7), vždy za předpokladu, že R je relace ekvivalence.
(a) Každé $x \in M$ patří do jedné třídy: protože R jako relace ekvivalence je speciálně reflexívní, platí xRx pro všechna $x \in M$, tj. $x \in K_x$ pro každé $x \in M$.
(b) Dvě různé třídy jsou disjunktní: Ukážeme, že dvě třídy, které nejsou disjunktní, musí být totožné.

1. krok: Nejsou-li K_x a K_y disjunktní, tak existuje alespoň jeden prvek $u \in K_x \cap K_y$. Pak platí $u \in K_x$ a $u \in K_y$, tedy podle definice tříd xRu a yRu. Díky symetrii R můžeme z (xRu a yRu) odvodit (xRu a uRy) a vzhledem k tranzitivitě R plyne odtud ihned xRy. Výsledek: nejsou-li K_x a K_y disjunktní, platí xRy,
2. krok: Abychom nyní ukázali $K_x = K_y$, dokažme, že každý prvek x' z K_x je také prvek z K_y, a obráceně, každý prvek y' z K_y je také prvek z K_x. Nechť nejdříve $x' \in K_x$, tj. xRx'. Podle 1. kroku platí xRy nebo, protože R je symetrická, také yRx, což spolu s xRx' dává yRx', tedy $x' \in K_y$. Je tudíž $K_x \subset K_y$. Je-li $y' \in K_y$, tj. yRy', můžeme z xRy (1. krok) díky tranzitivnosti R odvodit xRy', tj. $y' \in K_x$; je tedy také $K_y \subset K_x$, c. b. d.
(c) Žádná ze tříd není prázdná, protože $x \in K_x$ pro všechna $x \in M$.

Dokázali jsme tak, že každá relace ekvivalence R v M dává rozklad M, jehož třídami jsou podmnožiny $K_x = \{y: y \in M \text{ a } xRy\}$. K_x se proto nazývá třídou ekvivalence, resp. zbytkovou třídou x vzhledem k R, a množině $\{K_x\}_{x \in M}$ všech tříd ekvivalence říkáme *podílová množina M podle R*, stručně *podíl M podle R*, nebo *faktorová množina M podle R*; píšeme M/R. Protože každá třída ekvivalence je už jednoznačně určena svým libovolným prvkem, může každý prvek jako reprezentant zastupovat celou třídu. Vezmeme-li z každé třídy ekvivalence právě jednoho reprezentanta, dostaneme systém reprerentantů M/R.

Důkaz (2). Už prve jsme si rozmysleli, že každý rozklad M poskytuje příležitost definovat relaci ekvivalence R. Přitom platí xRy, právě když x patří do stejné třídy rozkladu jako y. Nyní se dá očekávat, že rozklad M, který dostaneme z R podle (1), bude opět počáteční rozklad $\mathfrak{Z}$ (a ne nějaký jiný rozklad $\mathfrak{Z}'$ množiny M).

Máme tedy ukázat, že $M/R = \mathfrak{Z}$, přičemž M/R sestává z tříd $K_x = \{y: y \in M \text{ a } xRy\}$. Označíme-li ty $\mathfrak{Z}$-třídy, které obsahují prvek $x \in M$, jako $K_{\mathfrak{Z}}(x)$, platí:

$$\begin{aligned} K_{\mathfrak{Z}}(x) &= \{y: y \in M \text{ a } y \text{ patří do stejné } \mathfrak{Z}\text{-třídy jako } x\} \\ &= \{y: y \in M \text{ a } x \text{ patří do stejné } \mathfrak{Z}\text{-třídy jako } y\} \\ &= \{y: y \in M \text{ a } xRy\} \text{ podle předchozí definice } R \\ &= K_x. \end{aligned}$$

$\mathfrak{Z}$-třída obsahující x tedy splývá pro každé $x \in M$ s M/R — třídou obsahující x, tj. rozklady $\mathfrak{Z}$ a M/R se skládají z týchž tříd. Platí tudíž, jak tvrdí věta, $\mathfrak{Z} = M/R$ a tím je náš důkaz dokončen.

Větu (2.4) můžeme také interpretovat takto: Mezi relacemi ekvivalence v množině M a rozklady M je vzájemně jednoznačné zobrazení; pro každou relaci ekvivalence R v M je množina tříd ekvivalence rozklad M a ke každému rozkladu M existuje relace ekvivalence v M, jejíž třídy ekvivalence jsou třídami tohoto rozkladu.

Relace ekvivalence jsou proto tak důležité, že tvoří základ každého (matematického) procesu abstrakce: Množina se vzhledem k relaci ekvivalence rozpadá na třídy prvků, jež jsou totožné vzhledem k jistému příznaku, a abstrahuje se od všech ostatních vlastností prvků, které pro existenci či neexistenci relace mezi libovolnými dvěma z nich nemají význam. Pak se na samotné třídy díváme jako na nové objekty, tj. přejdeme k podílové množině M/R. Podívejme se na několik příkladů:

(1) Obvyklá rovnost, třeba v množině celých čísel, je přirozeně relace ekvivalence, totiž už dříve zmíněná identita R_i, neboť je reflexívní, symetrická a tranzitivní. Není ostatně příliš zajímavá, protože každá třída ekvivalence sestává jen z jednoho prvku a podílová množina je totožná s výchozí množinou. Identita je jaksi „nej-

jemnější" relace ekvivalence, při ní žádné dva různé prvky nepadnou do téže třídy; neexistuje jemnější rozdělení M na třídy. „Nejhrubší" relace ekvivalence je naproti tomu zřejmě ta, při níž všechny prvky z M padnou do téže třídy, jestliže tedy existuje pouze jedna třída ekvivalence. Takto musí být každý prvek M ekvivalentní s každým prvkem M, tj. jedná se o totální relaci R_t. V tomto smyslu leží každá jiná relace ekvivalence „mezi" totální relací a identitou.

(2) V 7. třídě se zavádějí zlomky $\frac{a}{b}$ (a, b nezáporná celá čísla, $b \neq 0$) a mezi nimi se definuje podílová rovnost $=_Q$ vztahem

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

Ve škole se proto také říká: „Dva zlomky se rovnají, právě když se mohou převést na sebe krácením nebo rozšířením." Tato podílová rovnost je relací ekvivalence, neboť platí:

(a) $\frac{a}{b} =_Q \frac{a}{b}$, protože $ab = ab$; tj. $=_Q$ je reflexívní.

(b) $\frac{a}{b} =_Q \frac{c}{d} \Rightarrow ad = cb \Rightarrow cb = ad$ (neboť rovnost v N_0 je symetrická) $\Rightarrow \frac{c}{d} =_Q \frac{a}{b}$; tj. $=_Q$ je symetrická.

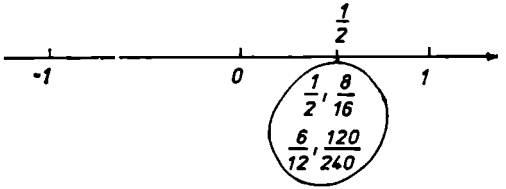
(c) $\left.\begin{array}{l} \frac{a}{b} =_Q \frac{c}{d} \Rightarrow ad = cb \Rightarrow adf = cbf \\ \frac{c}{d} =_Q \frac{e}{f} \Rightarrow cf = ed \Rightarrow cfb = edb \end{array}\right\} \Rightarrow$

$\Rightarrow adf = edb \Rightarrow af = eb \Rightarrow \frac{a}{b} =_Q \frac{e}{f}$;

tj. $=_Q$ je tranzitivní.

Na kterém místě důkazu používáme tranzitivitu rovnosti v N_0; kde se používá $d \neq 0$?

Množina M všech nezáporných zlomků se tudíž rozpadá vzhledem k relaci $=_Q$ na třídy zlomků s navzájem rovným podílem; podílová množina $M/=_Q$ je známa jako množina nezáporných racionálních čísel. Jako reprezentanta třídy ekvivalence z $M/=_Q$ vezmeme nejlépe zlomek, který se nedá dále krátit. Pro ilustraci tohoto rozkladu na třídy slouží obr. 22.

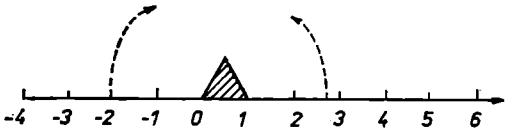


Obr. 22

(3) Další důležitá relace ekvivalence v množině Z celých čísel je kongruence modulo m (rovnost zbytků při dělení číslem m; píšeme $\equiv$ (mod m)). V odstavci 2.2 jsme už ukázali, že relace „dává při dělení třemi týž zbytek" je symetrická, tranzitivní a reflexívní, a na jednotlivých krocích důkazu se zřejmě nic nezmění, když místo s „3" pracujeme s „m". Přesto byste si zde měli tuto úvahu provést ještě jednou. Protože je tedy „$\equiv$" relace ekvivalence, rozpadá se množina Z celých čísel na třídy čísel s navzájem rovnými zbytky a třídy ekvivalence jsou třídy „stejných zbytků", z čehož vzniklo shora uvedené a na obecný případ přenesené označení „zbytková třída". Vezmeme-li $m = 3$, rozpadne se Z na tři třídy, totiž

$K_0 = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$
se zbytkem 0,

$K_1 = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$
se zbytkem 1,
$K_2 = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$
se zbytkem 2.



Obr. 23

Vytváření zbytkových tříd modulo 3 můžeme znázornit takto (obr. 23): Představme si číselnou osu jako nekonečné vlákno, které budeme „navíjet" kolem rovnostranného trojúhelníka o straně 1. Ve výchozí pozici zvolme za nulový bod číselné přímky jeden z vrcholů trojúhelníka a navíjejme „kladnou" a „zápornou" polopřímku kolem trojúhelníka proti sobě. Pak se ve vrcholech trojúhelníka sejdou právě všechny prvky patřící do téže třídy ekvivalence. Tento názorný výklad se dá přirozeně udělat i pro vytváření zbytkových tříd modulo 4, 5 atd.; stačí místo trojúhelníka vzít pravidelný čtyř- nebo pětiúhelník se stranou délky 1, atd.

(4) Je snadné, zjistit, že relace „rovnoběžný s" v množině přímek roviny je relací ekvivalence. Množina všech přímek roviny se tedy rozpadá na třídy navzájem rovnoběžných přímek a každé takové třídě říkáme směr. Na tomto příkladu je vidět, jak relace ekvivalence tvoří základ procesu abstrakce, zde pro vznik pojmu směr. Pokuste se naproti tomu objasnit pojem směru popisem!

(5) O soustavě dvou lineárních rovnic se dvěma neznámými (stejně dobře to ale může být m rovnic s n neznámými) říkáme, že je ekvivalentní s jinou soustavou

lineárních rovnic, právě když souhlasí jejich množiny řešení. Přitom mlčky předpokládáme, že obě soustavy uvažujeme ve stejném definičním oboru — třeba R. Ekvivalence soustav lineárních rovnic je zřejmě relace ekvivalence. Úlohu řešit soustavu lineárních rovnic můžeme také interpretovat takto: Utvořme, vycházející z dané soustavy, řetěz soustav lineárních rovnic, v němž je každá soustava ekvivalentní s předchozí, tak, abychom na konci tohoto řetězu dostali co nejjednodušší soustavu, jejíž řešení už můžeme bezprostředně určit. Tranzitivnost ekvivalence pak zaručuje, že také první soustava je s poslední ekvivalentní. Nalezli jsme tedy řešením poslední soustavy i řešení dané soustavy. Předvedeme to na jednoduché soustavě:

$$\begin{array}{l} 5x + y = 3 \\ 3x - 4y = 11 \end{array} \Leftrightarrow \begin{array}{l} 20x + 4y = 12 \\ 3x - 4y = 11 \end{array} \Leftrightarrow \begin{array}{l} 23x = 23 \\ 3x - 4y = 11 \end{array} \Leftrightarrow$$

$$\Leftrightarrow \begin{array}{l} x = 1 \\ 3x - 4y = 11 \end{array} \Leftrightarrow \begin{array}{l} x = 1 \\ 3.1 - 4y = 11 \end{array} \Leftrightarrow \begin{array}{l} x = 1 \\ -4y = 8 \end{array} \Leftrightarrow$$

$$\Leftrightarrow \begin{array}{l} x = 1 \\ y = -2 \end{array}$$

Z poslední soustavy rovnic bezprostředně čteme $L = \{(1; -2)\}$. Našli jsme tak i množinu řešení dané soustavy.

Jediný problém při řešení soustavy lineárních rovnic spočívá zřejmě v tom, že potřebujeme zjistit, které úpravy převádějí soustavu lineárních rovnic na soustavu s ní ekvivalentní, a ukázat, že prostřednictvím takových úprav můžeme libovolnou soustavu převést na jednoduchou konečným počtem kroků. Ve škole se takové ekvivalentní úpravy soustav lineárních rovnic probírají: změna pořadí rovnic; násobení jedné rovnice nenulovým číslem; přechod od jedné rovnice k součtu této rovnice s jinou rovnicí soustavy.

Ve větě (2.2) a v připojené poznámce o jejím obrácení jsme viděli, že pro reflexívní relaci platí:

R je symetrická a tranzitivní $\Leftrightarrow$ R splňuje rovnost třetímu. Podle toho můžeme relaci ekvivalence charakterizovat také jako reflexívní relaci, pro niž platí rovnost třetímu.

Doplňující úvahu, jak vypadá graf a uzlový graf relace ekvivalence, přenecháváme čtenáři.

U KUŘAT NEVLÁDNE ŘÁD

2.4 RELACE USPOŘÁDÁNÍ

Čtenář se dozví něco o relacích uspořádání a o jejich snášenlivosti s relacemi ekvivalence

Stejně jako je elementární potřeba člověka třídit objekty bytí a myšlení a prostřednictvím příznaků „rovnocennosti" je rozdělovat do tříd (relace ekvivalence), je elementární i jeho potřeba uspořádávat okolní svět, udávat stupnici hodnot. K tomu slouží takové relace jako „je větší než", „není těžší než", „je podmnožina", „je potomek", „stojí v abecedě před", „stal se dříve než"; tzv. relace uspořádání. Jakými vlastnostmi jsou tyto relace charakterizovány?

Čistě intuitivně bychom mluvili o uspořádání hodnot jen tehdy, je-li tranzitivní, tj. když platí: Stojí-li x v uvedeném uspořádání před y a y zase před z, tak musí také x stát před z. „Klovací seznam" u kuřat nemůžeme tedy považovat za uspořádání, neboť klove-li kuře Berta kuře Hertu, ale kuře Herta zas kuře Martu, není ještě jisté, že také kuře Berta klove kuře Martu. Mezi kuřaty tedy nevládne řád!

Relace „$\leqq$", resp. „$<$", které známým způsobem poskytují uspořádání hodnot v množině R reálných čísel,

jsou příkladem toho, že relace uspořádání může být jak reflexívní, tak i ireflexívní (jako „<“). Podle toho nazýváme relaci uspořádání reflexívní, resp. ireflexívní. Od uspořádání hodnot budeme ale muset požadovat ještě další vlastnost: Stojí-li v daném uspořádání x před y, nemůže zřejmě stát zároveň y před x; tento případ může nastat nejvýše tehdy, je-li $x = y$ a uvažovaná relace je reflexívní. Musíme tedy od reflexívní relace uspořádání požadovat, aby byla antisymetrická, a od ireflexívní relace uspořádání, aby byla asymetrická.

Při zběžném zkoumání jsme snadno ochotni ještě vyžadovat, aby pro dva různé prvky x, y vždy bylo x před y nebo y před x, což např. platí pro čísla vzhledem k relaci uspořádání „je větší než“ nebo pro lidi vzhledem k relaci uspořádání „není starší než“. Ale už pohled na relaci „je potomek“ ukazuje, že takové uspořádání nemusí nutně být „lineární“, nýbrž že se dané uspořádání může také rozvětvit do „rodokmenu“. Shrňme tyto předběžné úvahy v následující definici:

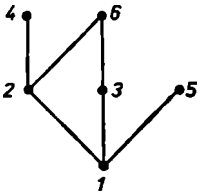
Definice 2.7. Relace R v M se nazývá *reflexívní relace uspořádání v* M, právě když je reflexívní, antisymetrická a tranzitivní; *ireflexívní relace uspořádání v* M, právě když je ireflexívní, asymetrická a tranzitivní.

Protože podle V(2.1) ireflexívní a tranzitivní relace je také nutně asymetrická, stačilo by v definici D(2.7) říci: R je ireflexívní relace uspořádání, právě když R je ireflexívní a tranzitivní.

Pro znázornění relace uspořádání je jistě výhodnější uzlový graf než graf kartézský, což je zřetelné už na našem standardním příkladu „je dělitel“ v množině $M = \{1, 2, 3, 4, 5, 6\}$. Po prozkoumání vlastností relace uspořádání jej můžeme ještě dále zjednodušit: R je buď reflexívní, nebo ireflexívní. V prvém případě neobsa-

huje žádný bod grafu relace R „kruhovou šipku", v druhém případě ji obsahuje každý jeho bod, tu bychom však chtěli na základě úmluvy odstranit. Reflexivitu či ireflexivitu relace R už proto na jejím grafu nepoznáme, a musíme ji uvést zvlášť.

Stejně jako z antisymetrie pro reflexívní relaci uspořádání, tak i pro ireflexívní relaci uspořádání R z asymetrie plyne, že pro různé prvky $x, y \in M$ nemůže nikdy současně platit xRy a yRx. Platí-li např. xRy a neexistuje žádné z, pro něž xRz a zRy, tj. y je „výše" než x a neexistuje žádný prvek z „mezi", můžeme vskutku názorně nazvat y horním sousedem x a x dolním sousedem y. Položíme-li pak také podle toho bod P_y uzlového grafu nad P_x, může ještě odpadnout šipka a postačí spojit P_x a P_y navzájem úsečkou. Dostaneme tak, např. pro relaci „je dělitel" v $M = \{1, \ldots, 6\}$, dále zjednodušený graf na obr. 24, kterému se říká *Hasseho graf*.



Obr. 24

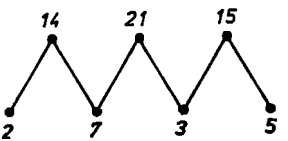
Shrňme ještě jednou, jak nakreslíme Hasseho graf relace uspořádání v konečné množině M: Začneme nejníže postavenými prvky, tj. těmi, které nejsou horním sousedem jiného prvku; v našem příkladu tedy 1. Na následujícím stupni budou stát všechny ty prvky M, které jsou horními sousedy nejníže položených prvků; v příkladu 2, 3, 5. Na n-tém stupni tohoto uspořádání budou stát ty prvky M, které jsou horními sousedy

prvků $(n-1)$-ního stupně. Úsečkami budou spojeny jen prvky sousedních stupňů, a sice x bude spojeno s y, právě když y je horním sousedem x. Pro různé prvky x a y na témže stupni neplatí ani xRy, ani yRx (proč?), nazývají se *nesrovnatelné*. Nesrovnatelné ale mohou být i dvojice prvků z různých stupňů, v příkladu třeba 5 a 6.

Neexistují-li v relaci uspořádání R v M nesrovnatelné prvky, tj. pro každé dva různé prvky nastane vždy jeden z případů xRy nebo yRx, nazývá se množina M *lineárně uspořádaná relací* R. Protože Hasseho graf takové lineárně uspořádané množiny leží na přímce, mluvíme také o *řetězci*. Řetězcem je např. množina R reálných čísel uspořádaných relací „$<$“ a obvyklá číselná osa je jejím Hasseho grafem, jen je zvykem ji kreslit vodorovně místo svisle.

Podíváme se nyní na několik příkladů relací uspořádání:

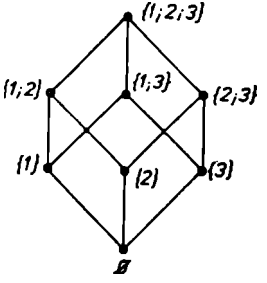
(1) Relace „je menší než“ v množině R reálných čísel je ireflexívní relace uspořádání, jak hned ověříme podle D(2.7). Přejdeme-li od relace „$<$“ k relaci „$\leqq$“, dostaneme reflexívní relaci uspořádání v R; přidáním identity můžeme takto vždy získat z ireflexívní relace uspořádání reflexívní relaci uspořádání. Stejně jako vzhledem k „$<$“, je R lineárně uspořádaná množina i vzhledem k „$\leqq$“.



Obr. 25

(2) Dělitelnost je reflexívní relace uspořádání v $\mathbb{N}_0 \setminus \{0\}$. Její reflexívnost, antisymetričnost a tranzitivnost jsme zjistili už v odstavci 2.2, a protože existují nesrovnatelné prvky (např. 2 a 3), není $\mathbb{N}_0 \setminus \{0\}$ lineárně uspořádaná. Obr. 25 ukazuje Hasseho graf relace dělitelnosti v množině $M = \{2, 3, 5, 7, 14, 15, 21\}$.

(3) Inkluze $\subset$ uvažovaná v potenční množině $\mathscr{P}(M)$ neprázdné množiny M je rovněž reflexívní relace uspořádání. Na obr. 26 je nakreslen Hasseho graf inkluze v $\mathscr{P}(\{1, 2, 3\})$.

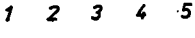


Obr. 26

(4) Množina slov německého jazyka je lineárně uspořádaná relací „stojí v abecedě před". Jak známo, stojí slovo I v abecedě před slovem II, jestliže ve slově I první písmeno zleva, v němž se obě slova liší, stojí v abecedě před odpovídajícím písmenem slova II. Přitom je ještě nutná úmluva týkající se přehlásek; často se s ö nakládá jako s oe, někdy však jednoduše jako s o. Jsou-li slova ve slovníku uspořádaná touto relací, říkáme, že jsou uspořádána *lexikograficky*.

(5) Na identitu R_i, o které už víme, že je relací ekvivalence, se můžeme také dívat jako na relaci uspořádání, neboť je reflexívní, tranzitivní a antisymetrická. Každé

dva různé prvky jsou vzhledem k R_i nesrovnatelné, tj. její Hasseho graf se skládá ze samých „izolovaných" bodů. Je znázorněn na obr. 27 pro množinu $M = \{1, 2, 3, 4, 5\}$.



Obr. 27

Nakonec ještě chceme prozkoumat spojitost mezi relací ekvivalence a relací uspořádání definovaných v téže množině — pro ilustraci sáhneme zpět pro příklad dřevěných tyček různých barev, délek a tvarů průřezu, zvolený v odstavci 2.3. Relace „má stejnou barvu jako" je relace ekvivalence a vede k rozdělení na třídy tyček stejné barvy. Relace „je delší než" vede k uspořádání tyček podle jejich délky. Platí-li pro dvě tyčky x a y „x je delší než y" a zaměníme-li x tyčkou x' stejné barvy (a y tyčkou y' téže barvy), nemůžeme tvrdit, že platí také „x' je delší než y'". Zde není žádná spojitost mezi oběma relacemi v tom smyslu, že by existence relace uspořádání mezi dvěma prvky dávala stejnou relaci mezi dvěma prvky s nimi ekvivalentními.

Vezměme naproti tomu relaci ekvivalence „dává stejný podíl" v množině nezáporných zlomků a tu relaci uspořádání, která je definována vztahem

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

(přesvědčte se sami, že se opravdu jedná o uspořádání), a zkoumejme, zda relace uspořádání zůstane zachována mezi dvěma zlomky se stejnými podíly. Je-li tedy $\frac{a'}{b'} =_Q \frac{a}{b}$, tj. $a'b = ab'$, a $\frac{c'}{d'} =_Q \frac{c}{d}$, tj. $c'd = cd'$,

pak vzhledem k $ad < cb$ platí taky $adb'd' < cbb'd'$. Je tedy $(ab')(dd') < (cd')(bb')$, takže $(a'b)(dd') < (c'd)(bb')$, a odtud dále plyne $a'd' < c'b'$, tj. $\frac{a'}{b'} <_Q \frac{c'}{d'}$.

Uspořádání dvou prvků z M zde tedy dává stejné uspořádání mezi všemi prvky jim ekvivalentními. Proto dává relace uspořádání v M zároveň i uspořádání v podílové množině M/R. V takovém případě říkáme, že relace uspořádání a ekvivalence jsou slučitelné.

Definice 2.8. Relace ekvivalence R v M a relace uspořádání S v M se nazývají *slučitelné*, právě když pro všechna $x, y, x', y' \in M$ platí:

$$(xSy \text{ a } xRx' \text{ a } yRy') \Rightarrow x'Sy'.$$

Píšeme-li místo R znak $\sim$ a místo S znak $<$, bude D(2.8) v dobře zapamatovatelné podobě znít takto:

$$(x < y \text{ a } x \sim x' \text{ a } y \sim y') \Rightarrow x' < y'.$$

2.5 CVIČENÍ

1. Následující relace v M zapište jako podmnožiny $M \times M$:
   a) „následuje bezprostředně za" v $M = \{0, 1, 2, 3, 4, 5\}$;
   b) „je vlastní podmnožinou" v $M = \mathcal{P}(\{1, 2, 3\})$;
   c) „je dělitelem" v $M = \{2, 4, 5, 8, 45, 60\}$.

2. Udejte všechny binární relace v $M = \{1; 2\}$ jako podmnožiny $M \times M$. Jaký je podle vás počet všech binárních relací v n-prvkové množině?

3. Nakreslete uzlový a kartézský graf následujících relací v $M = \{1, 2, 3, 4, 5, 6\}$:
   a) $R_1 = \{(x, y): xy \text{ je liché}\}$;
   b) $R_2 = \{(x, y): y = x + 2\}$.

4. Udejte příklad

a) tranzitivní relace, která není ani reflexívní, ani symetrická;

b) symetrické a tranzitivní relace, která není reflexívní;

c) dvou relací R, S, pro něž $R \subset S$ a $R \neq S$;

d) dvou navzájem inverzních relací.

5. a) Jaký je vztah mezi symetrickou relací a relací, která je sama k sobě inverzní?

b) Jakou vlastnost má relace R v M, pro niž platí $R_i \subset R$ (R_i je identita v M)?

c) Které relace jsou charakterizovány vztahem $R \circ R \subset R$?

6. Kdosi tvrdí, že symetrická a tranzitivní relace je vždycky také reflexívní, a odůvodňuje to takto: „Je-li R symetrická, platí spolu s xRy i yRx, odkud díky tranzitivitě hned plyne xRx. Takže R je také reflexívní". Cvičení 4b) už ukázalo, že tvrzení neplatí. Kde se ale v předchozím „odůvodnění" skrývá chyba?

7. Které z následujících relací jsou relace ekvivalence?

a) $R_1 = \{(x, y): x - y$ je celočíselný násobek tří$\}$ v N_0;

b) $R_2 = \{(a, a)\}$ v $M = \{a\}$;

c) relace „je dělitel" v N_0;

d) relace „je shodný s" v množině obrazců v rovině;

e) relace „má stejnou limitu jako" v množině konvergentních posloupností reálných čísel;

f) relace R v $\mathsf{N}_0 \times \mathsf{N}_0$, kde $(a, b)R(c, d)$, právě když $a + d = c + b$;

g) relace R_f v R, kde $R_f = \{(x, y): f(x) = f(y)\}$, přičemž f je libovolná funkce R do R.

Pro relaci f) určete třídu ekvivalence obsahující (2; 5).

8. Ukažte:

a) Je-li R reflexívní a tranzitivní relace v M, je $R \cap R^{-1}$ relace ekvivalence v M.

b) Pro relace ekvivalence R a S je i $R \cap S$ relace ekvivalence. Platí to i pro $R \cup S$?

9. a) Nakreslete Hasseho graf relace „je dělitel" v $M = \{2, 4, 5, 8, 45, 60\}$.

b) Ukažte na konkrétních příkladech, že výroky „všechny prvky $y \neq x$ z M leží nad x" (v daném uspořádání) a „v M neexistuje prvek, který by ležel pod x", nevyjadřují totéž.

10. Ukažte:

a) Je-li R (reflexívní, resp. ireflexívní) relace uspořádání v M, je také R^{-1} (reflexívní, resp. ireflexívní) relace uspořádání v M.

b) Je-li R, resp. S reflexívní relace uspořádání v M, resp. v N, je také relace T v $M \times N$, kde $(x_1, y_1)T(x_2, y_2) \Leftrightarrow$ $\Leftrightarrow x_1 R x_2$ a $y_1 S y_2$, reflexívní relace uspořádání.

11. a) Nechť M je neprázdná konečná množina, $\mathscr{P}(M)$ její potenční množina. Zjistěte, zda relace ekvivalence „má právě tolik prvků jako" je v $\mathscr{P}(M)$ slučitelná s inkluzí.

b) Za jakých předpokladů na funkci f je relace ekvivalence zkoumaná ve cvičení 7g) slučitelná s relací uspořádání „$\leqq$" v R?

3. OPERACE

$2 \circ 4 = 3$ a $7 \circ 17 = 12$?

3.1 POJEM OPERACE

Operace jako zobrazení — mnoho příkladů, některé už důvěrně známé, ale snad i nějaké méně známé

Tisková chyba? Početní chyba? Jistě uvažujete o správnosti rovností uvedených v nadpise, pokud máte na mysli základní početní operace v číselném oboru. K tomuto problému se ještě vrátíme.

Vedle sčítání, násobení, odčítání a dělení racionálních čísel jsme už poznali i další operace, např. tvoření průniku, sjednocení a rozdílu množin a skládání přiřazení. Na některé známé příklady se podíváme blíže:

Sčítání přirozených čísel	Odčítání zlomků
$(6; 7) \mapsto 13$	$(9; 7) \mapsto 2$
$(0; 8) \mapsto 8$	$(17; 0) \mapsto 17$
$(2; 9) \mapsto 11$	$(0{,}5; 9) \mapsto ?$

Průnik množin	Sjednocení množin
$(\{1; 2\}, \{3\}) \mapsto \emptyset$	$(\{a, b\}, \{c\}) \mapsto \{a, b, c\}$
$(\{7; 8\}, \{8; 9\}) \mapsto \{8\}$	$(\{a\}, \emptyset) \mapsto \{a\}$
$(\{7, 4, 0\}, \emptyset) \mapsto \emptyset$	$(\{a, b\}, \{a, b\}) \mapsto \{a, b\}$

Naše příklady ukazují, že „operační předpis" uspořádané dvojici prvků množiny M jednoznačně přiřazuje opět prvek z M. Operaci tedy můžeme chápat jako speciální zobrazení, přičemž vzory jsou uspořádané dvojice prvků množiny M a obrazy jsou prvky z M. Sčítání celých nezáporných čísel je zobrazení $N_0 \times N_0$ do N_0. Odčítání nezáporných racionálních čísel je zobrazení

z $\mathsf{Q}^+ \times \mathsf{Q}^+$ na Q^+, protože ne každé dvojici nezáporných racionálních čísel je přiřazen nějaký obraz. Průnik a sjednocení jsou zobrazení $\mathscr{P}(M) \times \mathscr{P}(M)$ na $\mathscr{P}(M)$.

Sestrojme ještě následující příklad: každé uspořádané dvojici celých nezáporných čísel (a, b) přiřaďme jako obraz číslo $(a + b)^2$. Také toto zobrazení můžeme chápat jako operaci. Protože ale jako obrazy nedostaneme všechna celá nezáporná čísla, nýbrž jen druhé mocniny, máme před sebou zobrazení $\mathsf{N}_0 \times \mathsf{N}_0$ do N_0.

Příklady nám naznačují, jak by asi měl být pojem operace v množině M definován:

Definice 3.1. Nechť M je neprázdná množina. Každé zobrazení φ z $M \times M$ do M se nazývá *binární operace v množině* M. Přiřazuje-li φ dvojici (a, b) jako obraz prvek c, píšeme místo $\varphi(a, b) = c$ také $a \circ b = c$. Množina M se nazývá *nosič operace*.

Protože operace jsou speciální zobrazení, mohli bychom mluvit o definičním oboru a oboru hodnot operace. Tak je např. definičním oborem dělení v množině R reálných čísel množina $\mathsf{R} \times (\mathsf{R} \setminus \{0\})$. Je-li definiční obor operace φ: $M \times M \to M$ roven $M \times M$, nazýváme φ *neomezeně definovanou operací*; platí-li $\mathscr{D}(\varphi) \subset M \times M$ a $\mathscr{D}(\varphi) \neq M \times M$, nazývá se φ *parciální operace*.

Pojem binární operace v množině M zavedený v D(3.1) se dá zobecnit dvěma směry. Přiřadíme-li prostřednictvím zobrazení φ každé uspořádané n-tici $(a_1, \ldots, a_n)$ prvků a_i množiny M prvek z M, mluvíme o n-ární operaci v množině M. V ještě obecnějším smyslu můžeme mluvit také o n-ární operaci, máme-li zobrazení z $M_1 \times \times M_2 \times \ldots \times M_n$ do M. Např. skalární součin dvou vektorů a „násobení" vektoru reálným číslem jsou takové binární operace, v nichž vystupují navzájem rozdílné množiny.

Také tvoření aritmetického průměru dvou racionálních čísel můžeme chápat jako neomezeně definovanou binární operaci:

$$(a, b) \mapsto c = \frac{a + b}{2}.$$

Tak se také dají vyložit rovnosti uvedené v nadpisu. Interpretujeme-li značku „$\circ$" jako symbol pro tvoření aritmetického průměru racionálních čísel, jsou uvedené rovnosti pravdivé výroky.

Při počítání s přirozenými čísly bychom teď chtěli používat sčítání jen na podmnožině S sudých čísel. Používáme přitom vlastně „novou" operaci „$+$", kterou můžeme chápat jako zobrazení z $S \times S$ do S. Jinak ovšem každý školák ví, že 2 a 4 je 6 bez ohledu na to, zda se na to díváme jako na sčítání celých čísel anebo jako na sčítání sudých čísel. Toto „nové" sčítání nazýváme zúžením sčítání celých čísel na množinu sudých čísel. Obecně se operace $\circ_A$ definovaná v množině A nazývá *zúžení operace* $\circ_B$ *definované v množině* B, právě když $A \subset B$ a pro libovolná $a, b \in A$ platí: $a \circ_A b = a \circ_B b$. Není však řečeno, že operace $\circ_A$, která je zúžením operace $\circ_B$ na množinu $A \subset B$, je v této množině A neomezeně definovaná operace. Zúžíme-li např. sčítání $+$ v N_0 na podmnožinu L lichých čísel, není $+_L$ neomezeně definovaná operace v L, neboť např. $3 \in L$, $5 \in L$, $3 + 5 = 8$, ale $8 \notin L$. Prvek 8 přiřazený dvojici $(3; 5)$ tedy už v množině L neleží. Naproti tomu zúžením operace sčítání v N_0 na množinu S sudých čísel se nedostaneme ven z množiny S, protože součet dvou libovolných sudých čísel je vždy zas sudý. Říkáme také, že S je *uzavřená vzhledem ke sčítání*.

Abychom získali představu o rozmanitosti operací, podívejme se ještě na některé důležité příklady:

Příklady. (1) V odstavci 1.7, příklad (2) jsme zavedli

zbytkové třídy celých čísel modulo m. Budeme je teď označovat $(0)_m$, $(1)_m$, ..., $(m-1)_m$. Protože zbytkové třídy jsou po dvou disjunktní neprázdné množiny, může každý prvek jednoznačně reprezentovat třídu, do které patří. Dohodněme se, že pro označení třídy budeme používat nejmenší nezáporné číslo v ní obsažené.
V množině zbytkových tříd celých čísel modulo 4 zaveďme „sčítání zbytkových tříd" a „násobení zbytkových tříd":

(1) $$(a)_4 + (b)_4 = (a + b)_4;$$
(2) $$(a)_4 . (b)_4 = (ab)_4.$$

Např. je

$$(3)_4 + (2)_4 = (5)_4 = (1)_4; \quad (2)_4 . (3)_4 = (6)_4 = (2)_4.$$

Uvědomte si, že symboly + a . mají různý význam. V rovnostech (1) a (2) bychom jako modul mohli také zvolit místo čtyřky libovolné celé kladné číslo. Definice operací v množině zbytkových tříd modulo m by pak byla dána vztahy (1′) $(a)_m + (b)_m = (a + b)_m$; (2′) $(a)_m . (b)_m = (ab)_m$. Sčítání a násobení zbytkových tříd jsme objasnili prostřednictvím „reprezentantů". Musíme ještě ukázat, že definice (1′) a (2′) mají smysl, a to tak, že dokážeme, že tyto operace „souhlasí" s tvořením zbytkových tříd. Vezměme místo a a b dva jiné reprezentanty $a' \in (a)_m$ a $b' \in (b)_m$, takže musí platit $a' + b' \in (a + b)_m$ a $a' . b' \in (ab)_m$. Dokážeme první z uvedených vztahů:
$a, a' \in (a)_m$ znamená, že $a = a' + rm$, a $b, b' \in (b)_m$ znamená, že $b = b' + sm$. Sečtením obou rovností dostaneme $a + b = a' + b' + (r + s)\, m$, tj. oba součty $a + b$ i $a' + b'$ leží ve stejné zbytkové třídě. Všech 16 možností aditivního (resp. multiplikativního) spojení zbytkových tříd modulo 4 lze zapsat pomocí tabulky (tabulky operace):

+	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(0)_4$	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(1)_4$	$(1)_4$	$(2)_4$	$(3)_4$	$(0)_4$
$(2)_4$	$(2)_4$	$(3)_4$	$(0)_4$	$(1)_4$
$(3)_4$	$(3)_4$	$(0)_4$	$(1)_4$	$(2)_4$

·	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(0)_4$	$(0)_4$	$(0)_4$	$(0)_4$	$(0)_4$
$(1)_4$	$(0)_4$	$(1)_4$	$(2)_4$	$(3)_4$
$(2)_4$	$(0)_4$	$(2)_4$	$(0)_4$	$(2)_4$
$(3)_4$	$(0)_4$	$(3)_4$	$(2)_4$	$(1)_4$

Přitom v levém krajním sloupci tabulky stojí levý sčítanec (resp. levý činitel) a v horním řádku pravý sčítanec (resp. pravý činitel).

(2) Ve skladovací hale opravárenského podniku používají k záznamu stavu různých náhradních dílů k určitému datu t_0 „číselný obdélník". Skládá se z n řádků a m sloupců, obsahuje tedy nm čísel. Každé z nich poskytuje informaci o tom, kolik náhradních dílů daného druhu je ve skladu k dispozici. Takový číselný obdélník se nazývá $n \times m$ *matice*; nm čísel a_{ik} nazýváme *prvky matice*. Znázorňujeme-li je pomocí proměnné, je použití dvojitého indexu účelné.

$$\begin{array}{l} \qquad\qquad\qquad\qquad \downarrow k\text{-tý sloupec} \\ i\text{-tý řádek} \rightarrow \begin{pmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1m} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \dots & a_{ik} & \dots & a_{im} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nm} \end{pmatrix} n \times m \text{ matice} \end{array}$$

První index i prvku a_{ik} matice A nazýváme *řádkovým indexem*. Udává, ve kterém řádku prvek stojí. Druhý index k, *sloupcový index*, vyjařuje, že a_{ik} patří do k-tého sloupce. Tak např. prvek a_{35} (čti: a-tři-pět) stojí v 3. řádku a 5. sloupci matice. Dvojice (n, m) přirozených čísel popisuje typ matice. Tak matice typu (4; 7) má právě 4 řádky a 7 sloupců. Matice budeme označovat velkými písmeny $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, ... Dvě matice $\mathbf{A} = (a_{ik})$ a $\mathbf{B} = (b_{ik})$ stejného typu (n, m) se rovnají, právě když se rovnají po

složkách, tj. právě když platí: $a_{ik} = b_{ik}$ pro $i \in \{1, 2, \ldots, n\}$ a $k \in \{1, 2, \ldots, m\}$. Takto definovaná rovnost matic je relace ekvivalence. Přírůstek a úbytek náhradních dílů, ke kterému dojde v určitém časovém období, může být právě popsán $n \times m$ maticí. Kladná čísla charakterizují přírůstek, záporná čísla úbytek a číslo nula značí, že nedošlo k žádným změnám. „Nový" stav v čase t_1 dostaneme zřejmě tak, že pro každý náhradní díl k původnímu počtu přičteme to číslo, které udává přírůstek, resp. úbytek tohoto dílu. To neznamená nic jiného, než že obě matice musíme sečíst následujícím způsobem:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1m} \\ b_{21} & b_{22} & \ldots & b_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ b_{n1} & b_{n2} & \ldots & b_{nm} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \ldots & a_{1m} + b_{1m} \\ a_{21} + b_{21} & a_{22} + b_{22} & \ldots & a_{2m} + b_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \ldots & a_{nm} + b_{nm} \end{pmatrix}, \qquad (3)$$

resp. ve zkrácené formě $(a_{ik}) + (b_{ik}) = (a_{ik} + b_{ik})$.
Zřejmě je součet dvou $n \times m$ matic, jejichž prvky jsou celá čísla, zase $n \times m$ matice celých čísel. Musíme si uvědomit, že (3) definuje součet matic jen pro matice stejného typu. Tak např. je

$$\begin{pmatrix} 2 & 1 & 7 \\ 5 & 3 & 0 \end{pmatrix} + \begin{pmatrix} 9 & -1 & 8 \\ -4 & 0 & 11 \end{pmatrix} = \begin{pmatrix} 11 & 0 & 15 \\ 1 & 3 & 11 \end{pmatrix}.$$

Naproti tomu matice

$$\begin{pmatrix} 2 & 1 \\ 3 & 0 \\ 4 & 7 \end{pmatrix} \text{ a } \begin{pmatrix} 2 & 1 & 9 & -3 \\ 5 & 1 & 8 & -4 \end{pmatrix}$$

se podle (3) sečíst nedají.

Problematika stavu zásob zprvu vyžadovala uvažovat jako prvky matice celá čísla. Upustíme-li od této věcné souvislosti, pak můžeme jako prvky matice připustit i racionální nebo reálná čísla. Matice, jejichž prvky jsou reálná čísla a mají tvar $1 \times m$, resp. $n \times 1$, nazýváme *řádkovým*, resp. *sloupcovým vektorem*. (3) tak kromě jiného definuje i součet takovýchto vektorů.

Nyní jsme blízko otázce, zda lze matice také „násobit". Otázku musíme nejdříve upřesnit: Můžeme definovat — vedle sčítání matic — maticovou operaci tak, aby byla účelná, tj. aby jednak mělo smysl použít ji při řešení problémů, jednak aby se „snášela" s už uvedeným sčítáním matic? Vyjděme opět z konkrétní problémové situace: V podniku se vyrábějí tři meziprodukty M_1, M_2 a M_3; pro každý z nich je potřeba určité množství surovin S_1 a S_2. Matice A poskytuje přehled o jejich spotřebě. Matice **B** charakterizuje, v jakém rozsahu se oba meziprodukty podílejí na výrobě obou konečných produktů K_1 a K_2.

$$\begin{array}{c} \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} M_1 & M_2 & M_3 \end{array} \\ \begin{pmatrix} 12 & 4 & 3 \\ 2 & 8 & 7 \end{pmatrix} \end{array} = \mathbf{A}, \qquad \begin{array}{c} \\ M_1 \\ M_2 \\ M_3 \end{array} \begin{array}{c} \begin{array}{cc} K_1 & K_2 \end{array} \\ \begin{pmatrix} 1 & 5 \\ 4 & 2 \\ 7 & 11 \end{pmatrix} \end{array} = \mathbf{B}.$$

Chceme-li nyní vědět, kolik jednotek suroviny S_1 je potřeba k výrobě konečného produktu K_1, pak zřejmě musíme sečíst součiny 12.1, 4.4 a 3.7. Odpovídajícím způsobem můžeme pro každý z obou konečných produktů určit spotřebu surovin vzhledem ke každé z nich zvlášť a výsledky zapsat do 2×2 matice. Data určená maticemi **A** a **B** k tomu plně dostačují. Záleží tedy jen na tom, abychom vhodně popsali operaci mezi maticemi **A** a **B**. Podle našeho příkladu dostáváme:

$$\begin{pmatrix} 12 & 4 & 3 \\ 2 & 8 & 7 \end{pmatrix} \cdot \begin{pmatrix} 1 & 5 \\ 4 & 2 \\ 7 & 11 \end{pmatrix} =$$

$$= \begin{pmatrix} 12.1 + 4.4 + 3.7 & 12.5 + 4.2 + 3.11 \\ 2.1 + 8.4 + 7.7 & 2.5 + 8.2 + 7.11 \end{pmatrix} =$$

$$= \begin{pmatrix} 49 & 101 \\ 83 & 103 \end{pmatrix} = \mathbf{C}\,.$$

Ze součinové matice **C** můžeme vyčíst spotřebu surovin. Uveďme si ještě jednou, že každý prvek **C** je součtem součinů některých prvků **A** a **B**. Abychom dostali prvek c_{ij} v i-tém řádku a j-tém sloupci matice **C**, musíme i-tý řádek **A** „vynásobit" j-tým sloupcem **B** (v tomto pořadí). Jak se tvoří každý z těchto součinů „řádek krát sloupec", si dobře zapamatujete z následujícího schématu:

$$(a_{i1}\ a_{i2} \ldots a_{im}) \cdot \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{mj} \end{pmatrix} = \left(\ldots \sum_{k=1}^{m} a_{ik} b_{kj} \ldots \right) = \begin{pmatrix} \vdots \\ \ldots\ c_{ij}\ \ldots \\ \vdots \end{pmatrix}$$

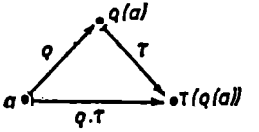
Tyto definice násobení matic můžeme zapsat také stručněji:

$$(a_{ik}) \cdot (b_{kj}) = \left(\sum_{k=1}^{m} a_{ik} b_{kj} \right) = (c_{ij}). \qquad (4)$$

Chceme-li $n \times m$ matici **A** násobit $r \times s$ maticí **B** podle (4), musí mít první činitel **A** právě tolik sloupců, kolik má druhý činitel **B** řádků, tj. musí být $m = r$. Matice **A**, **B** s touto vlastností nazveme *sdružené* (v tomto pořadí).

Vyjdeme-li opět z toho, že prvky matic jsou reálná čísla, je násobení ve (4) zavedeno pomocí sčítání a násobení reálných čísel. Ke vztahům mezi sčítáním a násobením matic dojdeme v odstavci 3.2.

(3) V odstavci 1.6 bylo objasněno skládání přiřazení. Je-li M libovolná neprázdná množina a T množina všech prostých zobrazení M na sebe, pak je skládáním prvků z T, tzv. transformací množiny M, dána neomezeně definovaná binární operace v T: Výsledkem složení dvou prvků ϱ a τ z T je takové zobrazení, které dostaneme, jestliže na každý prvek $a \in M$ provedeme nejprve ϱ a pak na obraz $\varrho(a)$ zobrazení τ.



Objasníme tento obecný postup na příkladech: Nechť M je konečná množina $\{1, 2, 3\}$. Pak se T skládá ze šesti zobrazení $\pi_1 = \begin{pmatrix}123\\123\end{pmatrix}$, $\pi_2 = \begin{pmatrix}123\\132\end{pmatrix}$, $\pi_3 = \begin{pmatrix}123\\213\end{pmatrix}$, $\pi_4 = \begin{pmatrix}123\\231\end{pmatrix}$, $\pi_5 = \begin{pmatrix}123\\312\end{pmatrix}$ a $\pi_6 = \begin{pmatrix}123\\312\end{pmatrix}$. Tato čísla v závorkách nejsou matice, jak jsme s nimi pracovali v příkladu 2, ale znázorňují tabulky hodnot. Složíme-li např. π_3 s π_5, dostaneme $\begin{pmatrix}123\\213\end{pmatrix} \cdot \begin{pmatrix}123\\312\end{pmatrix} = \begin{pmatrix}123\\132\end{pmatrix} = \pi_2$. Jako cvičení složte další zobrazení, např. π_2 a π_4, případně π_4 a π_2!

Obsahuje-li M právě n prvků $1, 2, \ldots, n$, skládá se T z $1.2 \ldots n = n!$ zobrazení množiny M na sebe. Každé možné pořadí $(i_1, \ldots, i_n)$ n různých prvků z M ve schématu $\begin{pmatrix}1 & 2 & \ldots & n\\ i_1 & i_2 & \ldots & i_n\end{pmatrix}$ popisuje totiž právě jeden prvek T. Každé prosté zobrazení konečné množiny M na sebe se nazývá *permutace.*

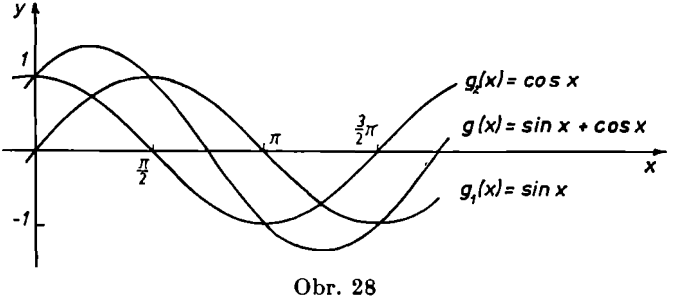
Nechť E je množina všech bodů roviny. Z množiny

všech prostých zobrazení E na sebe vyberme množinu všech shodností S. To jsou posunutí, otočení, osové souměrnosti nebo taková zobrazení, která dostaneme složením uvedených speciálních zobrazení. Zřejmě složením shodných zobrazení vznikne opět shodnost, to jste používali už ve škole. Skládáním shodností je na E dána neomezeně definovaná operace. Převádí-li shodnost ϱ obrazec Φ, tedy neprázdnou podmnožinu množiny E, na obrazec Φ', nazývají se Φ a Φ' *kongruentní (shodné)*.

(4) Budeme se zabývat množinou F všech funkcí reálné proměnné definovaných na intervalu $\langle a, b\rangle$ reálných čísel. V F zavedeme jako sčítání funkcí následující operaci označovanou $\oplus$:

$(f \oplus g)(x) = f(x) + g(x)$ pro libovolné $f, g \in F$ a pro všechna $x \in \langle a, b\rangle$. (5)

Sčítání funkcí je tedy zavedeno prostřednictvím sčítání funkčních hodnot — to jsou reálná čísla. Tato operace se užívá vždy, kdykoli jsou funkce aditivně spojeny. Tak můžeme např. $f(x) = mx + n$ chápat jako součet funkcí $f_1(x) = mx$ a $f_2(x) = n$, funkci $g(x) = \sin x + \cos x$ jako součet funkcí $g_1(x) = \sin x$ a $g_2(x) = \cos x$ (srov. obr. 28).



Obr. 28

Omezíme-li se na funkce, jejichž definiční obor je množina všech celých kladných čísel, tedy na posloupnosti reálných čísel, definuje (5) zároveň i sčítání číselných posloupností a často pak píšeme:

$$(a_n) \oplus (b_n) = (a_n + b_n) \text{ pro libovolné posloupnosti } (a_n), (b_n). \tag{5'}$$

Součet dvou posloupností (a_n) a (b_n) se tedy skládá z členů $a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n, \ldots$ Zajímavé je, že součet dvou konvergentních posloupností je vždy zas konvergentní posloupnost.

(5) Nakonec ještě spojíme dohromady několik dvojic operací. Už v odstavci 1.4 byly nápadné analogie mezi vlastnostmi operací $\bigcap$ a $\bigcup$. Ukazuje se, že shody takového druhu se mohou vyskytnout i u jiných dvojic.

Nechť $T = \{1, 2, 3, 4, 6, 12\}$ je množina všech celých kladných čísel, jež jsou děliteli čísla 12. Utvoření největšího společného dělitele (resp. nejmenšího společného násobku) dvou libovolných prvků z T dává vždy jednoznačně určený prvek z T, tj. v T jsou neomezeně definovány obě operace $a \wedge b = D(a, b)$ a $a \vee b = n(a, b)$. Už z porovnání tabulek obou operací lze učinit zajímavá odhalení.

V R byly tvořením maxima, resp. minima dvou reálných čísel zavedeny dvě operace $(a, b) \mapsto \max(a, b)$ a $(a, b) \mapsto \min(a, b)$. Každé uspořádané dvojici $(a, b) \in \mathsf{R} \times \mathsf{R}$ je operací „max", resp. „min" jako výsledek přiřazeno to z čísel a nebo b, které není menší, resp. není větší než to druhé. Jak jsme viděli, není snadné pro každou „novou" operaci nalézt nový spojovací znak. Často jsme sahali pro známé symboly (např. „.."), i když se nejednalo o operaci v číselném oboru. Tak budeme postupovat i napříště a nové spojovací znaky budeme používat jen tam, kde by mohlo dojít k záměně.

JE 17,2 % Z 93,6 ROVNO 93,6 % Z 17,2?

3.2 VLASTNOSTI OPERACÍ

Čtenář se seznámí s vlastnostmi operací; zjistí, za jakých podmínek je operace komutativní, asociativní, popřípadě invertibilní

Uvidíme, že otázku položenou v nadpisu je snadné zodpovědět. Počítáme-li totiž a procent z b, přičemž a a b jsou libovolné zlomky, pak je uspořádané dvojici (a, b) jednoznačně přiřazeno zlomek $\frac{ab}{100}$. Budeme počítání procent chápat jako operaci neomezeně definovanou na $\mathbb{Q}^*$, budeme pro ni užívat znaku % a psát $a \,\%\, b = \frac{ab}{100}$. Shora položenou otázku můžeme nyní převést na otázku obecnější, zda pro libovolné $a, b \in \mathbb{Q}^*$ platí $a \,\%\, b = b \,\%\, a$. Je-li výsledek nezávislý na pořadí „operandů", nazývá se operace komutativní.

Definice 3.2. Neomezeně definovaná operace $\circ$ na množině M se nazývá *komutativní*, právě když pro všechna $a, b \in M$ platí $a \circ b = b \circ a$.

Víme, že sčítání celých čísel a násobení zlomků patří mezi komutativní operace. Díky poslední skutečnosti se dá ukázat, že operace % je na $\mathbb{Q}^*$ komutativní: platí $a \,\%\, b = \frac{ab}{100} = \frac{ba}{100} = b \,\%\, a$ pro všechna $a, b \in \mathbb{Q}^*$. Tím je také zodpovězena otázka z nadpisu: Platí-li totiž $a \,\%\, b = b \,\%\, a$ pro všechny zlomky a a b, platí také $17{,}2 \,\%\, 93{,}6 = 93{,}6 \,\%\, 17{,}2$. Naproti tomu z rovnosti $2^4 = 4^2$ neplyne, že umocňování přirozených čísel

je komutativní operace; je přece možné hned uvést protipříklady.

Vyjmenujme teď několik dalších příkladů komutativních operací: Sčítání a násobení zbytkových tříd (srov. příklad 1 v odstavci 3.1) jsou operace s touto vlastností. Pro libovolné zbytkové třídy $(a)_m$, $(b)_m$ totiž platí:

$$(a)_m + (b)_m = (a + b)_m = (b + a)_m = (b)_m + (a)_m$$

a

$$(a)_m \cdot (b)_m = (ab)_m = (ba)_m = (b)_m \cdot (a)_m .$$

Protože sčítání a násobení zbytkových tříd bylo definováno pomocí sčítání a násobení celých čísel, je pochopitelné, že podáváme důkaz vlastností těchto operací se zbytkovými třídami odkazem na odpovídající vlastnosti operací na **Z**. Objasněme tento princip ještě na dalších příkladech:

Sčítání reálných funkcí definovaných na intervalu I je komutativní operace. Byla definována pomocí sčítání reálných čísel; platí proto $f \oplus g = g \oplus f$ pro libovolné funkce f a g z F díky rovnosti $(f \oplus g)(x) = f(x) + g(x) = g(x) + f(x) = (g \oplus f)(x)$ pro všechna $x \in I$. Snadno se můžeme přesvědčit, že komutativní je i sčítání posloupností reálných čísel (opět chápané jako speciální funkce s definičním oborem $\mathbf{N}_0$).

Podobně je komutativní sčítání matic stejného typu, zavedené v příkladu 2 odstavce 3.1, neboť platí:

$$(a_{ik}) + (b_{ik}) = (a_{ik} + b_{ik}) = (b_{ik} + a_{ik}) = \\ = (b_{ik}) + (a_{ik}) .$$

Násobení sdružených matic bylo sice definováno pomocí sčítání i násobení reálných čísel — obě operace jsou komutativní; domněnka, že na základě toho je také násobení matic komutativní, se však ukazuje jako nesprávná. Je-li třeba matice **A** typu (2; 3) a matice **B** typu

(3; 4), součin **AB** sice existuje, ovšem matice **B** a **A** se v tomto pořadí násobit nedají, poněvadž nejsou sdružené. I když se omezíme na čtvercové matice typu (n, n), je možno uvést protipříklady jako

$$\begin{pmatrix} 2 & 0 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix},$$

ale

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

Skládání transformací v množině M (srov. příklad 2 v odstavci 3.1) je obecně nekomutativní operace, jak ukazuje už složení dvou následujících permutací:

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

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

Můžeme ale dokázat komutativitu skládání pro speciální množiny transformací, např. pro množinu všech posunutí v rovině, nebo i pro množinu všech otočení kolem pevného bodu roviny.

Nakonec si ještě uvědomme, že všechny operace uvedené v příkladu 5 odstavce 3.1 jsou komutativní, neboť jistě platí $a \wedge b = b \wedge a$ pro všechna celá kladná čísla a, b a $\max(x, y) = \max(y, x)$ pro všechna reálná čísla x, y.

Že jsou obě operace $\cap$ a $\cup$ komutativní, bylo předvedeno už v odstavci 1.4. Máme-li zjistit průnik tří množin A, B a C, můžeme utvořit nejprve $A \cap B$ a pak průnik této množiny s množinou C. Ale můžeme také počítat průnik A s předem zjištěným průnikem $B \cap C$. Bylo by jistě zlé, kdyby oba postupy vedly k různým výsledkům. Tvrzení $(A \cap B) \cap C = A \cap (B \cap C)$ z věty V(1.2) nás však uklidňuje.

Je-li nějaká operace „nezávislá na uzávorkování jednotlivých prvků", jako např. i sjednocení množin nebo součet a násobení reálných čísel, nazývá se *asociativní*.

Definice 3.3. Operace $\circ$ v množině M se nazývá *asociativní*, právě když pro všechna $a, b, c \in M$ platí

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Zatímco u asociativní operace můžeme jednotlivé operandy libovolně spojovat a provádět na nich postupně danou operaci, u neasociativních operací musíme vždy dbát úmluvy, že pokud nejsou použity závorky, postupujeme při provádění operace jako při psaní zleva doprava. To znamená, že $9 - 5 - 3$ je totéž jako $(9 - 5) - 3$, což musíme odlišovat od $9 - (5 - 3)$.

Důkaz, že sčítání a násobení zbytkových tříd je asociativní, je poměrně jednoduchý. Také sčítání funkcí zavedené v příkladu 4 odstavce 3.1 má tuto vlastnost, neboť platí:

$$\begin{aligned}((f \oplus g) \oplus h)(x) &= (f \oplus g)(x) + h(x) = \\ &= (f(x) + g(x)) + h(x) = \\ &= f(x) + (g(x) + h(x)) = \\ &= f(x) + (g \oplus h)(x) = (f \oplus (g \oplus h))(x)\end{aligned}$$

pro libovolné funkce f, g a h a pro všechna $x \in I$.

Skládání permutací, otáčení nebo souměrností je asociativní, neboť dokonce skládání libovolných přiřazení má tuto vlastnost (srov. odstavec 1.6).

Prozkoumejme ještě některé operace uvedené v příkladu 5 odstavce 3.1. Asociativita $\cap$ a $\cup$ byla už ukázána v odstavci 1.4. Platí ale také

(1) $\max(a, \max(b, c)) = \max(\max(a, b), c)$ a
(2) $\min(a, \min(b, c)) = \min(\min(a, b), c)$.

V (1), resp. (2) je totiž v každém z obou výrazů určeno

to z čísel a, b, c, které není menší (resp. není větší) než každé z obou zbylých čísel.

Při důkazu asociativity „nejmenšího společného dělitele" je potřeba jednoznačně vyjádřit každé přirozené číslo jako součin mocnin prvočísel. Přirozené číslo n přitom píšeme jako součin mocnin všech prvočísel, přičemž je exponent roven nule, právě když příslušné prvočíslo není dělitelem čísla n. Kupříkladu je

$$14 = 2^1.3^0.5^0.7^1.11^0 \ldots,$$
$$20 = 2^2.3^0.5^1.7^0.11^0 \ldots,$$

přičemž ... naznačuje, že všechna další prvočísla vystupují v rozkladu s exponentem nula. Vystupuje-li v rozkladu na prvočinitele čísla a (resp. b) prvočíslo p s exponentem α_p (resp. β_p), obsahuje, jak známo, nejmenší společný dělitel $D(a, b)$ toto prvočíslo s exponentem $\min(\alpha_p, \beta_p)$. Platí tedy pro $a = \prod_{i \in N_0} p_i^{\alpha_i}$, $b = \prod_{i \in N_0} p_i^{\beta_i}$ a $c = \prod_{i \in N_0} p_i^{\gamma_i}$ také $D(D(a, b), c) = \prod_{i \in N_0} p_i^{\min(\min(\alpha_i, \beta_i), \gamma_i)} =$

$$= \prod_{i \in N_0} p_i^{\min(\alpha_i, \min(\beta_i, \gamma_i))} = D(a, D(b, c)),$$

přičemž jsme využili prve dokázanou asociativitu operace tvoření minima. Analogicky ukážeme, že také operace nejmenší společný násobek je asociativní, přičemž se využije (1).

Sčítání a násobení reálných čísel je jak komutativní, tak i asociativní; odčítání a dělení nemají žádnou z těchto vlastností. Přesto je domněnka, že komutativita a asociativita jsou navzájem související vlastnosti operace, nesprávná. Existují komutativní operace, jež nejsou asociativní, např. tvoření aritmetického průměru dvou reálných čísel, a asociativní operace, jež nejsou komutativní, např. skládání permutací.

Nepostačitelnost číselného oboru při počítání bývá často podnětem k jeho rozšíření. Zjistíme, že jisté rovnice v daném oboru nemají řešení. Tak např. v N_0 nejsou řešitelné ani všechny rovnice tvaru $a + x = b$, ani všechny rovnice tvaru $ay = b$ pro daná $a, b \in \mathsf{N}_0$. Říkáme tomu, že sčítání a násobení není v N_0 *invertibilní*, tj. dva sčítanci (činitelé) sice určují jednoznačně svůj součet (součin), obráceně se ale vždy nedá ze součtu a jednoho sčítance (součinu a jednoho činitele) určit druhý sčítanec (činitel).

Definice 3.4. Neomezeně definovaná operace $\circ$ na množině M se nazývá *invertibilní*, právě když pro libovolná a, $b \in M$ existují x a y z M taková, že platí $a \circ x = b$ a $y \circ a = b$.

Násobení v množině racionálních čísel různých od nuly je invertibilní operace. Naproti tomu násobení libovolných reálných čísel tuto vlastnost nemá, protože např. rovnice $0.x = 17$ nemá v R řešení. Vlastnost invertibility operace $\circ$ je totožná s požadavkem existence řešení rovnic uvedených v D(3.4), tj. operace $\circ$ je v M invertibilní, právě když každá rovnice $a \circ x = b$ a $y \circ a = b$ má v M alespoň jedno řešení.

Skládání transformací množiny M je invertibilní operace. Na důkaz ukažme pro dané transformace ϱ a τ řešení rovnice $\varrho.x = \tau$. Protože $\varrho(\varrho^{-1}.\tau) = (\varrho.\varrho^{-1}).\tau = \tau$, splňuje tuto podmínku $x = \varrho^{-1}.\tau$. Přitom je ϱ^{-1} inverzní zobrazení k ϱ a spolu s ϱ a τ jsou také ϱ^{-1} a $\varrho^{-1}.\tau$ prvky množiny T všech transformací M. Odpovídajícím způsobem se ukáže, že i každá rovnice $y.\varrho = \tau$ pro $\varrho, \tau \in T$ má v T řešení.

Proto je i skládání všech permutací konečné množiny M invertibilní.

Sčítání matic a sčítání funkcí jsou invertibilní operace.

Není obtížné tato tvrzení dokázat. Použije se pouze toho, že sčítání reálných čísel má tuto vlastnost.

Také sčítání zbytkových tříd je invertibilní operace, neboť každá rovnice $(a)_m + (x)_m = (b)_m$ má řešení $(x)_m = (b - a)_m$, protože pro daná celá čísla a a b má rovnice $a + x = b$ v $\mathbf{Z}$ vždy řešení, totiž $x = b - a$. Že násobení zbytkových tříd vzhledem k libovolnému modulu m invertibilní být nemusí, ukazuje následující protipříklad: Rovnice $(2)_4 . (x)_4 = (3)_4$ nemá v množině všech zbytkových tříd modulo 4 řešení, neboť jinak by muselo existovat celé číslo x takové, že $2x - 3 = 4c$ pro $c \in \mathbf{Z}$. Na levé straně této rovnice stojí ale liché číslo, zatímco na pravé straně vždy sudé číslo.

Také následující operace nejsou invertibilní. Důkaz dostaneme v každém jednotlivém případě nalezením rovnice, která v oboru příslušné operace nemá řešení. Překontrolujte to!

— Násobení čtvercových matic

$$\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & u \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}.$$

— Tvoření průniku množin $\{a, b, c\} \cap X = \{a, d\}$.

— Tvoření sjednocení množin $\{a, b\} \cup X = \{a\}$.

— Největší společný dělitel dvou čísel v množině všech dělitelů čísla 12 $D(4, x) = 6$.

— Nejmenší společný násobek dvou čísel v množině všech dělitelů čísla 12 $n(4, x) = 2$.

— Tvoření maxima, resp. minima dvou reálných čísel $\max(4, x) = 1$, $\min(x, 3) = 100$.

Existují invertibilní operace, jež nejsou komutativní, např. skládání transformací, a také invertibilní operace, jež nejsou asociativní, např. tvoření aritmetického

průměru dvou racionálních čísel. Vlastnost invertibility není tedy svázána ani s komutativitou, ani s asociativitou.

Z rovnosti $a + c = b + c$ můžeme usuzovat na $a = b$, tj. sčítanec c na obou stranách rovnosti smíme vyškrtnout. Také rovnost $ac = bc$, kde a, b, c jsou celá čísla, se dá zkrátit na $a = b$, pokud c je číslo různé od nuly.

Definice 3.5. Říkáme, že neomezeně definovaná operace $\circ$ na množině M má vlastnost *krácení*, právě když pro libovolná $a, b, c \in M$ současně platí (1) a (2):

(1) Z $a \circ c = b \circ c$ plyne $a = b$.
(2) Z $c \circ a = c \circ b$ plyne $a = b$.

Stejně jako komutativita a asociativita, je i možnost krácení vlastnost dané operace; proto nemůžeme přechod od $a \circ c = b \circ c$ k $a = b$ motivovat „dělením" obou stran rovnosti číslem c, tj. užitím další operace.

Pravidla vyjádřená v (1) a (2) definice D(3.5) se nazývají — ne příliš účelně — pravidla krácení, i když zřejmě s krácením zlomků nijak nesouvisejí.

Je jasné, že pro komutativní operace z podmínky (1) plyne podmínka (2), a obráceně, také podmínka (2) dává podmínku (1). Jak už zdůraznil předchozí příklad, z $a.0 = b.0$ neplyne $a = b$. Může tedy nastat případ, že operace nemá vlastnost krácení, přesto však jisté prvky jejího nosiče můžeme vždy „zkrátit". Říkáme pak, že takový prvek je *regulární*. Číslo nula je sice vůči sčítání racionálních čísel regulární, ne však vzhledem k násobení.

Zatímco invertibilita operace $\circ$ v množině M je totožná s podmínkou existence řešení lineárních rovnic, vlastnost krácení zaručuje jednoznačnost jejich řešení. Můžeme tedy vyslovit následující větu:

Věta 3.1. *Je-li operace* $\circ$ *definovaná v množině* M *invertibilní a má-li přitom vlastnost krácení, pak pro libovolná* $a, b \in M$ *má každá z rovnic* $a \circ x = b$ *a* $y \circ a = b$ *právě jedno řešení.*

Důkaz. Existence řešení je zaručena vlastností invertibility operace $\circ$; zbývá ukázat jednoznačnost. Předpokládejme, že $a \circ x = b$ má dvě různá řešení x_1 a x_2, takže z $a \circ x_1 = b$ a $a \circ x_2 = b$ díky rovnosti pravých stran plyne i rovnost levých stran: $a \circ x_1 = a \circ x_2$, a na základě vlastnosti krácení je $x_1 = x_2$ ve sporu s předpokladem. Analogicky se dokáže, že také každá rovnice $y \circ a = b$ má právě jedno řešení.

Skládání transformací množiny M, ale i sčítání zbytkových tříd, sčítání matic a funkcí jsou operace s vlastností krácení. Abychom to dokázali pro poslední tři jmenované operace, musíme využít skutečnosti, že sčítání celých čísel (resp. reálných čísel) má vlastnost krácení. Ukážeme to na příkladu sčítání funkcí definovaných na intervalu I: Podle předpokladu platí $f \oplus g = h \oplus g$, tedy pro všechna $x \in I$ $(f \oplus g)(x) = (h \oplus g)(x)$. Odtud plyne $f(x) + g(x) = h(x) + g(x)$, což je rovnost reálných čísel, tudíž $f(x) = h(x)$ pro všechna $x \in I$, tedy $f = h$.

Naproti tomu následující operace nemají vlastnost krácení, což dokážeme udáním protipříkladu:

— Násobení čtvercových matic:

$$\text{Je} \quad \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix},$$

$$\text{avšak} \quad \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix}.$$

— Tvoření průniku množin:

Je $\{a, c\} \cap \{a, b\} = \{a, d\} \cap \{a, b\}$,

avšak $\{a, c\} \neq \{a, d\}$.

— Násobení zbytkových tříd:

Je $(0)_4 . (2)_4 = (0)_4 . (3)_4$,

avšak $(2)_4 \neq (3)_4$.

— Nejmenší společný násobek v množině všech dělitelů čísla 12:

Je $n(3; 4) = n(6; 4)$,

avšak $3 \neq 6$.

— Tvoření maxima reálných čísel:

Je $\max(2; 17) = \max(1; 17)$,

avšak $2 \neq 1$.

Nyní už také jistě nebude obtížné najít příklady, jež ukazují. že největší společný dělitel dvou přirozených čísel, sjednocení množin stejně jako tvoření minima dvou reálných čísel nejsou operace s vlastností krácení.

Jestliže jsme až dosud uvažovali vlastnosti, jež se týkaly jen jedné operace, budou nás teď zajímat pravidla, kterým podléhá „souhra" dvou operací v množině M.

Definice 3.6. Na množině M nechť jsou neomezeně definovány dvě operace označené jako „násobení" $\circ$ a jako „sčítání" $\#$. Násobení se nazývá *distributivní vzhle-*

dem ke sčítání, právě když pro všechna $a, b, c \in M$ platí

$$a \circ (b \# c) = (a \circ b) \# (a \circ c)$$

a

$$(b \# c) \circ a = (b \circ a) \# (c \circ a).$$

Násobení v R je distributivní vzhledem ke sčítání, neboť platí $a(b + c) = ab + ac$ a $(b + c)\, a = ba + ca$, tj. smíme „odstranit závorky" a čísla „roznásobit". Naproti tomu sčítání není distributivní vzhledem k násobení. Formulace v D(3.6) také ukazuje, že vztah „je distributivní k" není symetrický.

V obou rovnostech v definici D(3.6) jsou na pravé straně užity závorky; to znamená, že nejdříve počítáme „součiny" a pak „součet součinů". To, že je při počítání s čísly můžeme vypustit, spočívá v úmluvě, že „násobení má přednost před sčítáním". Budeme tuto úmluvu přenášet i na jiné operace, pokud nebude hrozit nedorozumění.

Násobení zbytkových tříd se chová distributivně ke sčítání. Pro libovolné zbytkové třídy $(a)_m$, $(b)_m$, $(c)_m$ platí

$$(a)_m \cdot ((b)_m + (c)_m) = (a)_m \cdot (b + c)_m = (a(b + c))_m =$$
$$= (ab + ac)_m = (ab)_m + (ac)_m =$$
$$= (a)_m \cdot (b)_m + (a)_m \cdot (c)_m.$$

Rozmyslete si, které vlastnosti sčítání a násobení celých čísel se využily při tomto malém důkazu!

V příkladu 2 odstavce 3.1 bylo zavedeno sčítání a násobení matic na základě dvou různých problémů z oblasti ekonomie, k jejichž formulaci se obě operace hodily. Překvapuje proto, že obě tyto operace definované zdánlivě nezávisle jsou spolu svázány vlastností distributivnosti. Objasněme tuto skutečnost nejprve na speciálních příkladech 2×2 matic!

Pro libovolné matice **A**, **B** a **C** takové, že **B** a **C** jsou stejného typu a **A** a **B** jsou sdružené, platí

$$(a_{ik}).((b_{kj}) + (c_{kj})) = (a_{ik})\,(b_{kj} + c_{kj}) =$$
$$= (\sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj})) = (\sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj}) =$$
$$= (\sum_{k=1}^{n} a_{ik}b_{kj}) + (\sum_{k=1}^{n} a_{ik}c_{kj}) = (a_{ik}).(b_{kj}) + (a_{ik}).(c_{kj}).$$

Tím je dokázán jeden z obou požadavků D(3.6). Že násobení a sčítání splňuje i druhou rovnost, je možno ukázat analogicky.

Ve větě V(1.2) odstavce 1.4 bylo zdůrazněno, že operace $\cap$ a $\cup$ jsou dokonce navzájem distributivní. Je zajímavé, že takováto symetrie vzhledem k vlastnosti distributivnosti je i u obou dalších dvojic operací zavedených v příkladu 5 odstavce 3.1. Platí jak

$$D(a, n(b, c)) = n(D(a, b), D(a, c)),$$

tak i

$$n(a, D(b, c)) = D(n(a, b), n(a, c)),$$

$$\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c)),$$
$$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c)).$$

Důkazy přenecháváme čtenáři.

TĚŽKÁ ÚLOHA „MUŽE V ČERNÉM"

3.3 PRVKY SE SPECIÁLNÍMI VLASTNOSTMI
O neutrálních, pohlcujících a navzájem inverzních prvcích

Nemá vůbec lehkou úlohu, „muž v černém", jak se také často při kopané říká rozhodčímu — „neutrálu". Zatímco každý hráč může nasadit všechny své schopno-

sti a volní vlastnosti, aby svému mužstvu co nejvíce dopomohl k vítězství, musí se rozhodčí chovat neutrálně. Každé své rozhodnutí činí sám na základě pravidel, jeho možné sympatie či antipatie k jednomu mužstvu nesmějí ovlivnit vývoj utkání.

Sčítáme-li celá čísla, hraje roli „neutrála" nula. Pro libovolné celé číslo c platí $0 + c = c + 0 = c$, tj. číslo nula při sčítání ostatní čísla neovlivňuje. Proto také nazýváme nulu *neutrálním prvkem vzhledem ke sčítání celých čísel.*

Takové neutrální prvky najdeme i v jiných soustavách. Tak 1 se chová neutrálně při násobení racionálních čísel — jak známo, platí $1.a = a.1 = a$ pro všechna $a \in \mathbf{Q}$. 1 není ovšem neutrální vůči sčítání, stejně jako není nula neutrální vůči násobení. Muž, který je určen jako rozhodčí na zápasy kopané, se přece také může zúčastnit zápasu v házené jako hráč a rozhodně tam nemusí být neutrální.

Definice 3.7. Prvek n množiny M se nazývá *neutrální prvek vzhledem k neomezeně definované operaci* $\circ$ *na* M, právě když pro všechna $a \in M$ platí

$$a \circ n = n \circ a = a.$$

Platí-li $a \circ n = a$ (resp. $n \circ a = a$) pro všechna $a \in M$, nazývá se n *pravý neutrální* (resp. *levý neutrální*) *prvek operace* $\circ$.

Zřejmě je každý neutrální prvek zároveň pravý neutrální, tak i levý neutrální.

Pokusíme se vypátrat ještě další neutrální prvky: $(0)_m$, resp. $(1)_m$ jsou neutrální prvky v množině zbytkových tříd modulu m vzhledem ke sčítání, resp. vzhledem k násobení zbytkových tříd. Důkaz (jednoduchý) se vám jistě podaří. Využije se přitom skutečnost, že 0 (resp. 1)

je neutrální prvek vzhledem ke sčítání (resp. násobení) celých čísel.
Při sčítání matic stejného typu hraje roli neutrálního prvku, jak snadno nahlédneme, matice, jejíž prvky jsou vesměs nuly. Násobíme-li $n \times n$ matici $\mathbf{A}$ zleva $n \times n$ maticí

$$\mathbf{E} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

dostaneme $\mathbf{E}.\mathbf{A} = \mathbf{A}$, neboť při násobení i-tého řádku matice $\mathbf{A}$ k-tým sloupcem matice $\mathbf{E}$ dostaneme součet součinů, jež jsou vesměs rovny nule s výjimkou součinu $a_{ik}.1$. Také když násobíme matici $\mathbf{A}$ zprava maticí $\mathbf{E}$, dostaneme opět $\mathbf{A}$: platí jak $\mathbf{E}.\mathbf{A} = \mathbf{A}$, tak i $\mathbf{A}.\mathbf{E} = \mathbf{A}$, ačkoli jak známo, násobení matic není komutativní. Vyjasněte si působení matice $\mathbf{E}$ při násobení prozkoumáním příkladů, které si sami vyberete!
Tak jako v množině zbytkových tříd jsou i v množině $n \times n$ matic definovány dvě operace „sčítání" a „násobení". Vůči každé z obou operací existuje neutrální prvek. Pro lepší rozlišení se neutrální prvek vzhledem k aditivně popsané operaci také nazývá *nulový prvek* a vzhledem k multiplikativně popsané operaci *jednotkový prvek*; díky analogii s čísly 0 a 1 opravdu sugestivní označení pro neutrální prvky.
Identické zobrazení ι je prvek množiny T všech transformací množiny M. Je-li nyní φ libovolný prvek z T, platí jak $(\iota.\varphi)(a) = \varphi(\iota(a)) = \varphi(a)$, tak i $(\varphi.\iota)(a) = \iota(\varphi(a)) = \varphi(a)$ pro všechna $a \in M$, tj. $\iota.\varphi = \varphi.\iota = \varphi$. Je tedy ι neutrální prvek vzhledem ke skládání transformací množiny M.
V množině všech permutací tří prvků 1, 2, 3 může být

neutrální prvek znázorněn jako $\pi_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix}$, v množině všech posunutí roviny je to posunutí $\overrightarrow{PP}$ s nulovou „velikostí posunutí" a v množině všech otočení roviny kolem daného bodu je to otočení o nulový úhel. Vzhledem ke sčítání funkcí definovaných na intervalu I má vlastnost neutrálního prvku funkce n, kde $n(x) = 0$ pro všechna $x \in I$. Je-li totiž f libovolný prvek z množiny F těchto funkcí, tak pro všechna $x \in I$ platí: $(n \oplus f)(x) = n(x) + f(x) = 0 + f(x) = f(x)$, a tudíž $n \oplus f = f$, a protože víme, že operace $\oplus$ je komutativní, je také $f \oplus n = f$ pro všechna $f \in F$. Je tudíž také jasné, jak musí vypadat posloupnost, jež má hrát roli neutrálního prvku vzhledem ke sčítání posloupností reálných čísel. V potenční množině $\mathscr{P}(M)$ množiny M je množina M sama neutrálním prvkem vzhledem k operaci $\bigcap$ a prázdná množina $\emptyset$ je neutrální prvek vůči operaci $\bigcup$. Platí totiž $A \cap M = M \cap A = A$ a $A \cup \emptyset = \emptyset \cup A = A$ pro libovolnou množinu A z $\mathscr{P}(M)$ (srov. V(1.2)). Vám přenecháváme nalezení neutrálního prvku vzhledem k operacím $\wedge$ a $\vee$ zavedeným v množině všech dělitelů přirozeného čísla t a prozkoumání toho, zda existují neutrální prvky vůči operacím „tvoření maxima dvou reálných čísel", resp. „tvoření minima dvou reálných čísel" definovaných na R.

Není zajímavé hledat neutrální prvek vůči operaci $^0/_0$.

Uvažujme ještě, zda kromě 0 neexistuje ještě další neutrální prvek vzhledem ke sčítání celých čísel. To zřejmě nemůže nastat, neboť za předpokladu, že by existovalo $n \in \mathsf{Z}$, $n \neq 0$, rovněž s vlastností neutrálního prvku, plyne z rovnosti $n + a = a$ pro každé $a \in \mathsf{Z}$ ihned $n = a - a = 0$, což je ve sporu s předpokladem.

Můžeme to však dokázat ještě jinak: Předpokládejme, že n je spolu s nulou neutrální prvek vůči sčítání. Pak platí kromě $0 + n = n$ (1) také $0 + n = 0$ (2). Jednou

používáme toho, že 0 je neutrální prvek, podruhé, že n jako neutrální prvek při sčítání neovlivňuje žádný prvek, tedy ani nulu. Protože levé strany rovností (1) a (2) se rovnají, rovnají se i pravé strany. Je tedy $n = 0$, tj. vzhledem ke sčítání v Z existuje právě jeden neutrální prvek. Srovnáním obou myšlenkových postupů zjistíme, že jsme v prvém důkazu zahrnutím odčítání celých čísel užili více pomocných prostředků než v druhém důkazu. Protože jsme ve druhé úvaze vůbec nepoužili vlastností sčítání celých čísel, můžeme tento postup použít i na libovolnou operaci $\circ$. Tím je dokázáno, že operace v množině M nemůže mít více než jeden neutrální prvek.

Obě shora uvedené úvahy dovolují ještě další důsledek: Má-li operace $\circ$ jak pravý neutrální prvek n_P, tak i levý neutrální prvek n_L, musejí se díky rovnostem $n_L \circ n_P = n_L$ (působení pravého neutrálního prvku) a $n_L \circ n_P = n_P$ (působení levého neutrálního prvku) oba prvky shodovat. Pro operaci $\circ$ mohou tedy nastat jen následující případy:

— má pravý a nemá levý neutrální prvek,
— má levý a nemá pravý neutrální prvek,
— nemá ani levý, ani pravý neutrální prvek,
— má právě jeden neutrální prvek.

V množině F všech funkcí tedy kromě funkce $n(x) = 0$ pro všechna $x \in I$ neexistuje žádný další neutrální prvek vzhledem ke sčítání a identické zobrazení je jediný neutrální prvek vzhledem ke skládání transformací. Ve zkoumaných příkladech nenastal případ, že by operace měla jen pravý, ale nikoli levý neutrální prvek. Odčítání nezáporných celých čísel je takovou operací, neboť platí sice $a - 0 = a$ pro všechna $a \in \mathsf{N}_0$, neexistuje však prvek $n \in \mathsf{N}_0$ s vlastností $n - a = a$ pro libovolné $a \in \mathsf{N}_0$.

Neutrální prvek tedy neovlivňuje při provádění ope-

race ostatní prvky. Mohou se ale vyskytnout i speciální prvky, jež se vůči operaci chovají právě obráceně: Pozorujeme-li chování nuly při násobení reálných čísel, zjistíme, že tento prvek „pohlcuje" všechna ostatní čísla: Pro každé reálné číslo x platí $0.x = x.0 = 0$.

Definice 3.8. Prvek a množiny M se nazývá *agresívní prvek vzhledem k operaci* $\circ$ *definované na* M, právě když pro všechna $x \in M$ platí

$$a \circ x = x \circ a = a.$$

Prázdná množina $\emptyset$ v $\mathscr{P}(M)$ vystupuje jako agresívní prvek, uvažujeme-li ji vzhledem k operaci $\cap$, a množina M má tuto vlastnost vzhledem ke sjednocení (srov. V(1.2)). V množině $M = \{1, 2, 3, 4, 6, 12\}$ je číslo 1 agresívní prvek vůči tvoření největšího společného dělitele. Takový prvek můžeme v M najít i pro operaci nejmenšího společného násobku.

Má-li množina M vzhledem k asociativní operaci $\circ$ zavedené na M neutrální prvek n, pak je operace $\circ$ invertibilní, právě když jsou pro každý $a \in M$ řešitelné speciální rovnice $a \circ x = n$ a $y \circ a = n$. Je-li totiž $\circ$ invertibilní, jsou řešitelné všechny rovnice tvaru $a \circ x = b$ a $y \circ a = b$, tím spíše tedy i uvedené rovnice. A naopak, jsou-li tyto speciální rovnice řešitelné, jejich řešení označme např. $x = \bar{a}_P$, $y = \bar{a}_L$; pak můžeme hned dostat i řešení obecných rovnic: $a \circ x = b$ má řešení $x = \bar{a}_P \circ b$ a $y \circ a = b$ má řešení $y = b \circ \bar{a}_L$. Provedeme zkoušku: $a \circ x = a \circ (\bar{a}_P \circ b) = (a \circ \bar{a}_P) \circ b = n \circ b = b, y \circ a = (b \circ \bar{a}_L) \circ a = b \circ (\bar{a}_L \circ a) = b \circ n = b$.

Má tedy smysl ptát se na řešení — závisející zřejmě jen na a — rovnic $a \circ x = n$, resp. $y \circ a = n$. Kupříkladu ke každému celému číslu c přísluší v $(\mathbb{Z}, +)$ jako řešení rovnic $c + x = 0$ a $y + c = 0$ celé číslo $-c$ a v $(\mathbb{R} \setminus \{0\}, .)$ je racionálnímu číslu $r \neq 0$ rovnicí $r.x = x.r =$

$= 1$ přiřazeno racionální číslo $x = \frac{1}{r}$. Číslu 0 však tímto způsobem nemůžeme přiřadit žádné racionální číslo, protože rovnice $0.x = x.0 = 1$ nemá řešení.

Definice 3.9. Nechť $\circ$ je operace definovaná v množině M a nechť n je neutrální prvek vzhledem k $\circ$.
Prvek $\bar{a} \in M$ se nazývá *inverzním prvkem k a vzhledem* k $\circ$, právě když platí

$$(*) \qquad a \circ \bar{a} = \bar{a} \circ a = n.$$

Platí-li $a \circ \bar{a} = n$ (resp. $\bar{a} \circ a = n$), nazývá se $\bar{a}$ *pravý inverzní* (resp. *levý inverzní*) *prvek k a vzhledem k* $\circ$.

Zřejmě je $\bar{a}$ inverzní prvek k a, právě když je jak pravý, tak i levý inverzní prvek k a. U komutativních operací pojmy „pravý inverzní" a „levý inverzní" splývají.

Úvodní příklady vedou k domněnce, že k prvku a existuje nejvýše jeden inverzní prvek. Správnost této domněnky dokážeme pro asociativní operace v odstavci 4.2.

Díky symetrii rovností (*) vystupují prvky a a $\bar{a}$ zcela rovnoprávně, tj. je-li $\bar{a}$ inverzní prvek k a, je také a inverzní prvek k $\bar{a}$.

Prvek $\bar{a}$ inverzní k a často označujeme jako a^{-1} (resp. $-a$ při aditivním způsobu psaní); záměny s mocninou a^{-1} se nemusíme obávat, jak se později ukáže.

Chceme-li pátrat po dalších dvojicích navzájem inverzních prvků, musíme se omezit na zkoumání takových operací, jež mají neutrální prvek. V množině zbytkových tříd modulo 4 najdeme vzhledem ke sčítání ke každému prvku právě jeden takový, že jejich součet dá zbytkovou třídu $(0)_4 : (0)_4 + (0)_4 = (0)_4$, $(1)_4 + (3)_4 = (3)_4 + (1)_4 = (0)_4$ a $(2)_4 + (2)_4 = (0)_4$.

Naproti tomu neexistuje zbytková třída modulo 4, jež by byla řešením rovnice $(2)_4.(x)_4 = (1)_4$, tj. zbytková

třída $(2)_4$ nemá vzhledem k násobení zbytkových tříd inverzní prvek. Každá $n \times m$ matice (a_{ik}) má vůči sčítání matic inverzní prvek, totiž matici $(-a_{ik})$, neboť zřejmě platí

$$(a_{ik}) + (-a_{ik}) = (a_{ik} + (-a_{ik})) = (0).$$

V množině všech $n \times n$ matic existují jak prvky, jež vzhledem k násobení matic mají inverzní prvek, tj. inverzní matici, tak i takové prvky, pro něž žádnou inverzní matici nenajdeme. Podívejme se na dva příklady: K matici $\mathbf{A} = \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}$ je inverzní matice $\mathbf{A}^{-1} = \begin{pmatrix} 1/3 & -1/3 \\ 1/3 & 2/3 \end{pmatrix}$; platí $\mathbf{A}.\mathbf{A}^{-1} = \mathbf{A}^{-1}.\mathbf{A} = \mathbf{E}$. Přesvědčte se o tom! K matici $\mathbf{B} = \begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix}$ naproti tomu neexistuje inverzní matice. To se dá snadno ověřit, zkusíme-li vyřešit maticovou rovnici

$$\begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

jež vede na soustavu čtyř lineárních rovnic o čtyřech neznámých a, b, c, d. Má-li matice $\mathbf{A}$ inverzní matici, nazývá se *regulární*, jinak se $\mathbf{A}$ nazývá *singulární matice*. Mezi singulární matice patří mimo jiné ty, jež obsahují řádky nebo sloupce se samými nulami, a takové, u nichž je řádek, resp. sloupec, násobkem jiného řádku, resp. sloupce, což byl případ shora uvedeného příkladu.

Vůči skládání transformací existuje ke každému prvku prvek inverzní. Můžeme ukázat, že inverzní prvek k posunutí je posunutí, inverzní prvek k otočení okolo bodu P_0 je otočení okolo P_0, inverzní prvek ke shodnosti je shodnost.

Zatímco vzhledem ke sčítání funkcí ke každé funkci

existuje inverzní prvek, např. je $f(x) = -3x + \sin x$ a $g(x) = 3x - \sin x$ taková dvojice, pro operace uvedené v příkladu 5 odstavce 3.1 najdeme prvky, jež tuto vlastnost nemají. Tak v množině všech dělitelů čísla 12 neexistuje vzhledem k největšímu společnému děliteli inverzní prvek ke 4. Rovnice $\{a, b, c\} \cup X = \emptyset$ nemá v $\mathcal{P}(M)$ řešení, neexistuje tam tedy množina, jež by byla vůči $\cup$ inverzní k množině $\{a, b, c\}$. Nebude pro vás obtížné zkonstruovat další takové příklady.

RESPEKT SE VYPLÁCÍ

3.4 RELACE KONGRUENCE

Čtenář se dozví, za jakých podmínek relace ekvivalence respektuje operace a jak můžeme přirozeným způsobem definovat operaci mezi třídami rozkladu

Každé celé kladné číslo n patří buď do množiny P prvočísel, nebo do množiny P' složených čísel. $\mathbb{N}_0 \setminus \{0\}$ se tak rozpadá na dvě třídy P a P'. Ověřme na příkladech, jak je tento rozklad $\mathfrak{Z}$ množiny $\mathbb{N}_0 \setminus \{0\}$ respektován sčítáním přirozených čísel:

$$2 + 3 = 5, \quad 12 + 1 = 13, \quad 7 + 6 = 13,$$
$$3 + 5 = 8, \quad 4 + 6 = 10, \quad 11 + 9 = 20.$$

Zjišťujeme, že součet dvou prvočísel může být prvek jak P, tak i P'; také součet dvou složených čísel může být jak prvek P, tak i P'. Přičteme-li konečně prvočíslo ke složenému číslu, může zas součet ležet v kterékoli z obou tříd. Náš rozklad sčítání celých kladných čísel vůbec nerespektuje. Zdalipak respektuje alespoň násobení?

Zvolme jiný rozklad množiny $\mathbb{Z}$ celých čísel — rozdělme ji na třídu K_z záporných čísel, třídu K_k kladných čísel a třídu K_0, jež obsahuje jen nulu. Prověřme teď

chování tohoto rozkladu vůči sčítání. Součet dvou záporných čísel je sice vždy záporný, součet dvou kladných čísel vždy kladný a součet dvou prvků z K_0 vždy prvek z K_0, ale jakmile se při sčítání setkají prvky různých tříd, mohou se vyskytnout „nedisciplinovanosti“:

$$-3 + 2 = -1 \in K_z, \quad -3 + 4 = 1 \in K_k,$$
$$-3 + 3 = 0 \in K_0.$$

Zatímco náš rozklad nedostatečně respektuje sčítání, násobení se podřizuje, neboť pro libovolné $a, b \in \mathbf{Z}^+$, platí:

$$(+a).(-b) \in K_z, \quad 0.(+a) \in K_0, \quad 0.0 \in K_0,$$
$$(-a).(+b) \in K_z, \quad (+a).0 \in K_0,$$
$$(-a).(-b) \in K_k, \quad 0.(-a) \in K_0,$$
$$(+a).(+b) \in K_k, \quad (-a).0 \in K_0.$$

Příslušnost součinu dvou celých čísel do jedné třídy závisí tedy jen na příslušnosti jednotlivých činitelů do té které třídy, a ne na speciální volbě činitelů uvnitř dané třídy.

Vraťme se nakonec ještě jednou k rozkladu množiny $\mathbf{Z}$ všech celých čísel na zbytkové třídy podle relace ekvivalence „kongruentní (mod m)“. V příkladu 1 odstavce 3.1 bylo už ukázáno, že sčítání celých čísel je tvořením zbytkových tříd, resp. příslušnou relací ekvivalence respektováno: Pro $a', a'' \in (a)_m$ a $b', b'' \in (b)_m$ leží ve stejné zbytkové třídě také $a' + b'$ a $a'' + b''$, totiž v $(a + b)_m$. Za stejných předpokladů dostaneme pro $a' \equiv a''$ (mod m) a $b' \equiv b''$ (mod m), tj. $a' = a'' + gm$ a $b' = b'' + hm$, vynásobením obou posledních rovností

$$a'b' = a''b'' + m(a''h + b''g + mgh), \text{ tj.}$$
$$a'b' \equiv a''b'' \text{ (mod } m).$$

Leží-li tedy jak a' a a'', tak i b' a b'' ve stejných zbytkových třídách, platí totéž i pro $a'b'$ a $a''b''$. Relace

ekvivalence „kongruentní (mod m)“ v Z má tedy tu vlastnost, že respektuje sčítání a násobení celých čísel; takovou relaci nazýváme relace *kongruence*.

Definice 3.10. Relace ekvivalence R v množině M se nazývá *relace kongruence v struktuře* $(M, \circ)$, právě když relace R respektuje operaci $\circ$, tj. když pro všechna $a, b, a', b' \in M$ platí:

$$\text{Z } aRa' \text{ a } bRb' \text{ plyne } (a \circ b)R(a' \circ b').$$

Respekt se vyplácí! Tato snášenlivost relace „kongruentní (mod m)“ vůči sčítání, resp. násobení celých čísel dovoluje definovat v množině zbytkových tříd přirozeným způsobem novou operaci. V příkladu 1 odstavce 3.1 jsme to už předvedli: zbytkové třídy tvoří nosič nové operace. Dvě zbytkové třídy sčítáme, resp. násobíme tak, že v každé z obou tříd zvolíme libovolné celé číslo (reprezentanta) a ta sečteme, resp. vynásobíme. Každé celé číslo, které takto dostaneme, určuje jednoznačně a nezávisle na reprezentantu zbytkovou třídu, která je podle definice součtem, resp. součinem daných zbytkových tříd. Tímto způsobem jsou definovány operace v podílové množině $\mathbf{Z}/R$, která je vytvořena relací ekvivalence „kongruentní (mod m)“; množina $\mathbf{Z}/R$ tak získává strukturu: ze $(\mathbf{Z}, +, .)$ a R dostáváme $(\mathbf{Z}/R, +, .)$.

Shora uvažovaný rozklad množiny Z na třídy K_z, K_0, K_k je odvozen z relace ekvivalence, jež se ukázala jako snášenlivá vůči násobení celých čísel. Můžeme proto podle stejného principu v množině $\{K_z, K_0, K_k\}$ zavést násobení $\circ$ pomocí reprezentantů (viz tabulku).

$\circ$	K_z	K_0	K_k
K_z	K_k	K_0	K_z
K_0	K_0	K_0	K_0
K_k	K_z	K_0	K_k

Znovu abstrahujeme: Je-li relace ekvivalence R v M zároveň relací kongruence v $(M, \circ)$, můžeme mezi třídami ekvivalence podílové množiny M/R definovat operaci $\odot$ prostřednictvím reprezentantů:

$$K_x \odot K_y = K_z \Leftrightarrow x \circ y = z.$$

Přirozeně můžeme místo x, y zvolit i jiné reprezentanty x', y' z tříd ekvivalence K_x, K_y; to, že R je relace kongruence, naručuje, že součin $x' \circ y' = z'$ určitě zas patří do třídy K_z.

$(M/R, \odot)$ nazýváme *podílovou strukturou*, *faktorovou strukturou*, a nebo také *strukturou zbytkových tříd* $(M, \circ)$ vzhledem k R.

Už v příkladu 1 odstavce 3.1 jsme zjistili, že se mnohé vlastnosti operace $\circ$ v M přenášejí na operaci $\odot$ v M/R. Vysvětlení pro to najdeme v následujících odstavcích.

3.5 CVIČENÍ

1. Zjistěte, zda zúžení sčítání číselných posloupností na podmnožiny M_i $(i = 1, 2, 3)$ je neomezeně definovaná operace.
   a) M_1: množina všech aritmetických posloupností;
   b) M_2: množina všech geometrických posloupností;
   c) M_3: množina všech rostoucích posloupností.

2. Přesvědčte se, zda operace $\circ_1$ a $\circ_2$ definované následujícími tabulkami jsou komutativní či invertibilní a zda mají neutrální prvek.

$\circ_1$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\circ_2$	a	b	c	d
a	d	b	c	a
b	b	b	b	b
c	c	b	d	c
d	a	b	c	d

3. Dokažte:
$\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c))$
a
$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$.

4. Nechť $\circ_3$ je operace v $\mathbf{N}_0 \setminus \{0\}$, která číslům $a \neq 0$, $b \neq 0$ přiřazuje číslo, jež dostaneme zapsáním číslic obou čísel a a b za sebe (příklad: $a = 14$, $b = 156$, $a \circ_3 b = 14\,156$). Ukažte, že $\circ_3$ je asociativní, ale není komutativní. Zjistěte, zda $\circ_3$ je invertibilní a zda má vlastnosti krácení. Obsahuje množina $\mathbf{N}_0 \setminus \{0\}$ vůči $\circ_3$ levý (pravý) neutrální prvek?

5. V množině E všech bodů roviny je definována následující operace: jestliže $P \neq Q$, je $P \triangle Q$ třetí vrchol T rovnostranného trojúhelníka PQT značeného v matematicky kladném smyslu; v případě $P = Q$ položme $P \triangle Q = P$. Zjistěte, zda $\triangle$ je komutativní, asociativní či invertibilní. Má $\triangle$ vlastnost krácení?

6. Následující „tvoření průměrů" dvou čísel můžeme chápat jako operace:
aritmetický průměr racionálních čísel
$$a \circ_4 b = \frac{a + b}{2};$$
geometrický průměr nezáporných reálných čísel
$$a \circ_5 b = \sqrt{ab};$$
harmonický průměr kladných reálných čísel
$$a \circ_6 b = \frac{2ab}{a + b}.$$
Zjistěte, zda jsou tyto operace komutativní, asociativní či invertibilní a zda je mezi nimi operace s vlastností krácení. Dokažte, že žádná z uvedených operací nemá neutrální prvek a že každý prvek je vůči těmto operacím idempotentní, tj. že platí $a \circ_4 a = a \circ_5 a = a \circ_6 a = a$ pro všechna vhodná a.

7. Dokažte asociativitu operací $\wedge$ a $\vee$ využitím vztahu: $a = b \Leftrightarrow a \mid b$ a $b \mid a$.

8. Které z následujících operací mají levý, které pravý a které oboustranný neutrální prvek?
$a \uparrow b = a^b$ v $\mathbf{N}_0$, $a \square b = |a - b|$ v $\mathbf{Q}^*$,
$a \circ b = a + b - 7$ v $\mathbf{Z}$.

9. Má-li operace vlastnost krácení, nemusí ještě být invertibilní. Doložte to na příkladu operace $a \uparrow b = a^b$ v $\mathbf{N} \setminus \{1\}$.

10. Jsou dány následující objekty s operacemi (množina a operace):

a) $(\mathbf{Z}, \circ)$, $a \circ b = a - b$,
b) $(\mathbf{N}_0, \circ)$, $a \circ b = a^b$,
c) $(\mathbf{Z}, \circ)$, $a \circ b = 2a + b$,
d) $(\mathbf{Z}, \circ)$, $a \circ b = a + b - ab$,
e) $(\mathbf{N}_0, \circ)$, $a \circ b = a$,
f) $(\mathbf{N}_0, \circ)$, $a \circ b = 0$.

Zjistěte, které operace jsou komutativní a které asociativní. Dokažte: operace v b), d), e) a f) nejsou invertibilní a v c) je jednoznačně řešitelná každá rovnice $a \circ x = c$, ale už ne každá rovnice $y \circ b = c$ je řešitelná. Pro které operace existuje neutrální prvek?

11. Je dán obdélník se středem M a osami souměrnosti g_p a g_q. Nechť m je středová souměrnost se středem M a p, resp. q osová souměrnost s osami g_p, resp. g_q, n nechť je identické zobrazení. Sestavte tabulku skládání těchto zobrazení obdélníka na sebe.
Spočítejte $p.p.q.n.m.n.q.m.p$ na základě úvah a prostřednictvím tabulky. Řešte soustavu rovnic

$$x.y = p,$$
$$y.x^2.q = m.y^2.$$

Jaká zajímavá pravidla jste objevili při počítání s těmito speciálními zobrazeními?

12. Řešte maticovou rovnici $\mathbf{AX} + \mathbf{BX} = \mathbf{C} + \mathbf{D}$, kde $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 1 & -2 \\ -1 & 0 \end{pmatrix}$, $\mathbf{C} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\mathbf{D} = \begin{pmatrix} 1 & -3 \\ 0 & 2 \end{pmatrix}$. Jaké vlastnosti maticových operací se využijí při řešení? Které z matic jsou regulární?

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

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

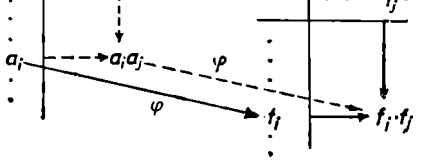
zjistíme, že se v nich počítá úplně stejně. Dokonce bychom mohli sestavit abstraktní počtní tabulku a podle toho, zda budeme prvky a_1, a_2, a_3, a_4 interpretovat jako čtyři funkce f_1, ..., f_4, nebo jako čtyři matice $\mathbf{A}_1$, ..., $\mathbf{A}_4$ (a odpovídajícím způsobem operaci . jednou jako 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.:

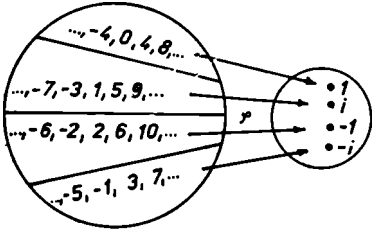
$$\left.\begin{array}{l}(G_1, \circ_1) \text{ grupa;}\\ (G_2, \circ_2) \text{ množina s operací;}\\ (G_1, \circ_1) \text{ izomorfní s } (G_2, \circ_2)\end{array}\right\} \Rightarrow (G_2, \circ_2) \text{ rovněž grupa.}$$

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.)

ZÁVĚREČNÁ POZNÁMKA

Ačkoliv název naší knížečky slibuje, že „každý začátek je snadný", pro čtenáře, jenž ji pozorně a s poctivým úsilím prostudoval až k tomuto místu, to může být mnohdy i četba obtížná. Ale jak se říká, „bez práce nejsou koláče", a úspěšný čtenář může s oprávněnou hrdostí říci, že se dopracoval k začátkům algebry.

Jsou to ovšem jen začátky, těžko můžeme čekat více od knížky tak skromného rozsahu, uvážíme-li, kolik generací matematiků pracovalo při stavbě budovy algebry. Čtenář mohl jen jakoby nahlédnout klíčovou dírkou. Ale přece jen — něco vidí. I když ji nemůže vidět v celé její rozloze, přece jen pozná jak základy, tak i některé podstatné obrysy této budovy.

A ještě více: našemu pozornému čtenáři jsme dali do ruky klíč, který mu může otevřít dveře k algebře, neboť algebraické myšlení, mnohé základní metody důkazu a technika při zkoumání struktur a konstrukci takových objektů, bohaté možnosti užití algebraických myšlenek při pořádání a systemizaci známých matematických skutečností, ale i při výzkumu souvislostí nových se dají naučit už při studiu základů algebry. V tomto smyslu si přejeme, aby co nejvíce čtenářů dostalo chuť na ještě více algebry, aby použili onen klíč a ještě trochu dále pootevřeli dveře do budovy jejích myšlenek.

VÝSLEDKY CVIČENÍ

Kapitola 1

1. $M_1 = \{x: x \in \mathbf{Q} \text{ a } |x| > 2\}$,
$M_2 = \{x: x \in \mathbf{Z} \text{ a } x^2 = 1\}$,
$M_3 = \{x: x \in \mathbf{Q} \text{ a } \frac{22}{7} < x < \pi\} = \emptyset$.

2. Průnikem je množina, která obsahuje jediný bod (2; 1).

3.

A	B	$A \cap B$	$A \cup (A \cap B)$
1	1	1	1
1	0	0	1
0	1	0	0
0	0	0	0

Porovnáním 1. a 4. sloupce dostáváme tvrzení a); b) dokážeme analogicky.

4. Z $A \subset B \subset C$ plyne $A \cup B = B$ a $B \cap C = B$, je tedy $A \cup B = B \cap C$.
Obráceně, z $A \cup B = B \cap C$ plyne, že $A \cup B \subset B$; leží tedy každé $x \in A$ také v B. Z uvedeného předpokladu ale dostaneme i $B \cap C \supset B$, tj. každé $x \in B$ leží také v C.

5. Jsou-li A_i, A_k disjunktní, tedy $A_i \cap A_k = \emptyset$, plyne tvrzení bezprostředně z toho, že $A \cap \emptyset = \emptyset$. Obrácené tvrzení neplatí, jak se snadno přesvědčíme konstrukcí protipříkladu.

6. Všechny výroky jsou navzájem ekvivalentní.

7. Nechť $x \in A \cup B$, pak je $x \in A$ nebo $x \in B$. V obou případech dostáváme $x \in Z$, je tedy $A \cup B \subset Z$.

8. Pravdivé jsou výroky c) a d).

9. a) $A \cap C$, b) $A \cap B$, c) A, d) $A \cap B$, e) $\emptyset$.

10. $A \times B$ má rs prvků.

11. Je-li $x \in A$ a $y \in C$, tj. $(x, y) \in A \times C \subset B \times C$, je také $x \in B$, neboli $A \subset B$. Stejně dostaneme i obrácenou inkluzi, tudíž $A = B$[13]).

12. F_1, F_2 a F_4 jsou zobrazení, pouze F_4 je vzájemně jednoznačné.

13. Hledané funkce můžeme popsat následujícími vztahy:
$(f \circ f)(x) = x^4 + 2x^2 + 2$, $(g \circ g)(x) = 9x + 8$,
$(f \circ g)(x) = 3x^2 + 5$, $(g \circ f)(x) = 9x^2 + 12x + 5$,
$f^{-1}(x) = \sqrt{x - 1}$, $g^{-1}(x) = \frac{1}{3}(x - 2)$.

14. Pouze c) a d) jsou rozklady.

15. Uvedené rozdělení je rozklad. To plyne z toho, že víme o podobných zobrazeních:
(1) složením dvou podobností dostaneme podobnost;
(2) inverzním zobrazením k podobnosti je podobnost;
(3) identické zobrazení je podobnost.

16. Jenom M_3 a M_6 jsou konečné množiny.

17. Vzájemně jednoznačné zobrazení φ množiny všech kmenových zlomků na $N_0 \setminus \{0\}$ můžeme definovat takto:

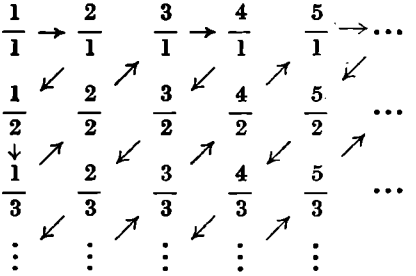
$$\varphi\left(\frac{1}{n}\right) = n .$$

Pro důkaz druhého tvrzení použijte návodu ke cvičení 18.

18. Očíslujme zlomky po řadě tak, jak ukazuje následující

[13]) Předpoklad $C \neq \emptyset$ je podstatný, neboť klademe $A \times \emptyset = \emptyset$ pro libovolnou množinu A. (Pozn. překl.)

schéma. Dostaneme tak vzájemně jednoznačné zobrazení Q^* na N_0.



Takovéto zobrazení můžeme použít i na množinu všech uspořádaných dvojic přirozených čísel.

Kapitola 2

1. a) $\{(1; 0), (2; 1), (3; 2), (4; 3), (5; 4)\}$.
   b) Označme $M_1 = \{1\}$, $M_2 = \{2\}$, $M_3 = \{3\}$, $M_4 = \{1; 2\}$, $M_5 = \{1; 3\}$, $M_6 = \{2; 3\}$, pak je
   $R = \{(\emptyset, M_1), (\emptyset, M_2), (\emptyset, M_3), (\emptyset, M_4), (\emptyset, M_5), (\emptyset, M_6), (\emptyset, M), (M_1, M_4), (M_1, M_5), (M_1, M), (M_2, M_4), (M_2, M_6), (M_2, M), (M_3, M_5), (M_3, M_6), (M_3, M), (M_4, M), (M_5, M), (M_6, M)\}$.
   c) $R = \{(2; 2), (2; 4), (2; 8), (2; 60), (4; 4), (4; 8), (4; 60), (5; 5), (5; 45), (5; 60), (8; 8), (45; 45), (60; 60)\}$.

2. $M \times M = \{(1; 1), (1; 2), (2; 1), (2; 2)\}$. Označíme-li $a = (1; 1)$, $b = (1; 2)$, $c = (2; 1)$ a $d = (2; 2)$, dají se všechny relace v M znázornit takto:
   $R_1 = \emptyset$, $R_2 = \{a\}$, $R_3 = \{b\}$, $R_4 = \{c\}$, $R_5 = \{d\}$, $R_6 = \{a, b\}$, $R_7 = \{a, c\}$, $R_8 = \{a, d\}$, $R_9 = \{b, c\}$, $R_{10} = \{b, d\}$, $R_{11} = \{c, d\}$, $R_{12} = \{a, b, c\}$, $R_{13} = \{a, b, d\}$, $R_{14} = \{a, c, d\}$, $R_{15} = \{b, c, d\}$, $R_{16} = M \times M$.

Každá relace v M je podle definice podmnožina $M \times M$. Existuje tedy tolik relací v M, kolik je podmnožin množiny $M \times M$. Obsahuje-li M n prvků, má $M \times M$ n^2 prvků a $\mathcal{P}(M \times M)$ má podle 1. kapitoly 2^{n^2} prvků.

3. $R_1 = \{(1; 1), (1; 3), (1; 5), (3; 1), (3; 3), (3; 5), (5; 1), (5; 3), (5; 5)\}$,
$R_2 = \{(1; 3), (2; 4), (3; 5), (4; 6)\}$.
Nyní můžeme uzlový či kartézský graf uvedených relací nakreslit.

4. a) např. relace „$<$" v N_0,
b) např. $R = \{(1; 1), (1; 2), (2; 1), (2; 2)\}$ v $M = \{1, 2, 3\}$,
c) $R \subset S$ a $R \neq S$ platí např. pro relaci R: „je vlastní dělitel" a S: „je dělitel" v N_0,
d) relace „bezprostředně následuje po"
a „stojí bezprostředně před" jsou příkladem navzájem inverzních relací v N_0.

5. a) Vždy platí $(x, y) \in R \Rightarrow (y, x) \in R^{-1}$. Je-li $R = R^{-1}$, pak je pro $(x, y) \in R$ také $(y, x) \in R$, tj. R je symetrická. Je-li obráceně R symetrická, platí $R = R^{-1}$, neboť všechny předchozí implikace lze obrátit. Jsou tedy výroky „R je symetrická" a „$R = R^{-1}$" ekvivalentní.
b) $R_i \subset R$ znamená, že pro všechna $x \in M$ platí $(x, x) \in R$, takže R je reflexívní. Obráceně, pro reflexívní R platí $R_i \subset R$.
c) Je-li $(x, y) \in R$ a $(y, z) \in R$, pak platí $(x, z) \in R \circ R$ (skládání přiřazení). Je-li nyní $R \circ R \subset R$, znamená to tranzitivitu R. Obráceně, z tranzitivity R vyplývá výrok $R \circ R \subset R$.
Předchozí výsledky můžeme shrnout:
R reflexnívní $\Leftrightarrow R_i \subset R$; R symetrická $\Leftrightarrow R = R^{-1}$;
R tranzitivní $\Leftrightarrow R \circ R \subset R$.

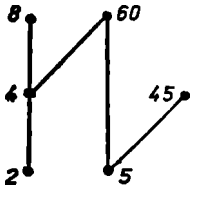
6. „Odůvodnění" začíná předpokladem, že pro prvek x existuje (alespoň) jedno y takové, že xRy; tj. uvedený závěr

je možný jen pro taková x, která jsou v relaci s nějakým prvkem $y \in M$. Abychom dostali reflexivitu, museli bychom mít xRx pro všechna x (z M).

7. Až na relaci c) jsou všechny relace reflexívní, symetrické a tranzitivní, tedy relace ekvivalence. Relace v c) není symetrická.
Třída ekvivalence relace f), která obsahuje prvek (2; 5), je $\{(x, x + 3): x \in \mathsf{N}_0\}$.

8. a) Podle V (2.3) se reflexivita a tranzitivita přenáší z R na R^{-1}; je tedy také $R \cap R^{-1}$ reflexívní a tranzitivní. Kromě toho je $R \cap R^{-1}$ symetrická:
$(x, y) \in R \cap R^{-1} \Rightarrow (x, y) \in R$ a $(x, y) \in R^{-1} \Rightarrow (y, x) \in R^{-1}$ a $(y, x) \in R \Rightarrow (y, x) \in R \cap R^{-1}$.
b) Protože $(x, x) \in R$ a $(x, x) \in S$ pro všechna $x \in M$, je také $(x, x) \in R \cap S$; tj. $R \cap S$ je reflexívní. Je-li $(x, y) \in R \cap S$, je $(x, y) \in R$ a $(x, y) \in S$ a na základě předpokládané symetrie R a S odtud plyne $(y, x) \in R$ a $(y, x) \in S$, neboli $(y, x) \in R \cap S$. Je tedy $R \cap S$ také symetrická, a podobně se ukáže, že je tranzitivní.
Pro $R \cup S$ to neplatí, jak ukazuje protipříklad $R = \{(a, a), (a, b), (b, a), (b, b)\}$, $S = \{(a, a), (a, c), (c, a), (c, c)\}$ pro $b \neq c$: $R \cup S$ obsahuje (b, a) a (a, c), ale neobsahuje (b, c), nemůže tedy být tranzitivní, a tudíž ani relací ekvivalence.

9. a)



b) Z grafu v cvičení 9a) vidíme, že výrok „v M neexistuje prvek, který by ležel pod 5" je pravdivý, zatímco „všech-

ny prvky $y \neq 5$ jsou nad 5" pravdivý není, neboť 2 a 5 jsou nesrovnatelné.

10. a) Tvrzení dostaneme použitím V(2.3). Protože některé zde použité výroky z V(2.3) nebyly v odstavci 2.2 dokázány, doženěte to zde!
b) Platí xRx pro všechna $x \in M$ a ySy pro všechna $y \in N$, podle definice T je tedy také $(x, y)T(x, y)$ pro všechny $(x, y) \in M \times N$. T je tedy reflexívní. Ze vztahů

$$(x_1, y_1)T\ (x_2, y_2)\ \text{a}\ (x_2, y_2)T(x_3, y_3)$$

plyne x_1Rx_2 a x_2Rx_3 stejně jako y_1Sy_2 a y_2Sy_3. Předpokládaná tranzitivita R a S dovoluje závěr, že x_1Rx_3 a y_1Sy_3, tedy také $(x_1, y_1)T(x_3, y_3)$. T je tudíž tranzitivní, a antisymetrie T se ukáže stejně.

11. a) Relace slučitelné nejsou; v $\mathscr{P}(\{1, 2, 3, 4\})$ např. platí: $\{1; 2\} \subset \{1, 2, 3\}$, $\{1, 2\}$ má právě tolik prvků jako $\{3; 4\}$ a $\{1, 2, 4\}$ právě tolik prvků jako $\{1, 2, 3\}$, ale neplatí $\{3; 4\} \subset \{1, 2, 4\}$.
b) Pro $x \leqq y$ musí být každý prvek úplného vzoru x při f menší nebo rovný každému prvku úplného vzoru y při f. Tuto podmínku kupříkladu splňuje funkce $f(x) = [x]$ ($[x]$ je největší celé číslo $\leqq x$).

Kapitola 3

1. Zúžení sčítání číselných posloupností na množiny M_1 a M_2 je neomezeně definovaná operace, neboť součet dvou aritmetrických (resp. rostoucích) posloupností je opět aritmetická (resp. rostoucí) posloupnost. Pro geometrické posloupnosti tento výrok neplatí.

2. Obě operace jsou komutativní, ale jenom $\circ_1$ je invertibilní. Např. rovnice $b \circ_2 x = c$ nemá v $\{a, b, c, d\}$ řešení. Neutrálním prvkem uvedených operací je a, resp. d.

8. Důkaz můžeme provést probráním všech možných případů, jež mohou vzhledem k relaci $\leqq$ pro a, b, c nastat.

4. Psaní číslic přirozených čísel za sebou je nezávislé na uzávorkování: je tedy $\circ_3$ asociativní. Příklad $12 \circ_3 45 = 1\,245 \neq 4\,512 = 45 \circ_3 12$ ukazuje nekomutativnost $\circ_3$. Operace $\circ_3$ není ani invertibilní, neboť např. rovnice $1\,467 \circ_3 x = 347$ nemá zřejmě řešení. Naproti tomu má $\circ_3$ vlastnost krácení; z $a \circ_3 x_1 = a \circ_3 x_2$ vždy plyne $x_1 = x_2$, neboť rovnají-li se dvě přirozená čísla, rovnají se i příslušné číslice (v téže číselné soustavě). Pravý nebo levý neutrální prvek operace $\circ_3$ nemá.

5. Operace $\triangle$ není ani komutativní, ani asociativní, ale je invertibilní. Také má vlastnost krácení.

6. Všechny tři operace jsou komutativní, zato není žádná z nich asociativní. $\circ_4$ je invertibilní, $\circ_5$ a $\circ_6$ invertibilní nejsou, což lze doložit neřešitelností rovnic $0 \circ_5 x = 9$, resp. $3 \circ_6 x = 6$. Vlastnost krácení mají $\circ_4$ a $\circ_6$; $\circ_5$ ji nemá, neboť z rovnosti $\sqrt[]{0.x_1} = \sqrt[]{0.x_2}$ nevyplývá nutně $x_1 = x_2$. Že žádná z operací nemá neutrální prvek, dokážeme nepřímo, idempotence se ověří výpočtem.

7. Návod: Nechť $t_1 = D(a, D(b, c))$ a $t_2 = D(D(a, b), c)$, pak platí $t_1 | a$ a $t_1 | D(b, c)$, tj. t_1 dělí a, b i c, platí tedy také $t_1 | D(a, b)$ a $t_1 . c$, odkud plyne $t_1 | t_2$. Právě tak ukážeme, že $t_2 | t_1$. Ze vztahů $t_1 | t_2$ a $t_2 | t_1$ však plyne (v N) $t_1 = t_2$.

8. $\uparrow$ má 1 jako pravý neutrální prvek, nemá ale levý neutrální. 0 je neutrální prvek $\square$ a -7 je neutrální prvek $\circ$.

9. Z $a^{x_1} = a^{x_2}$, resp. $y_1^a = y_2^a$ plyne $x_1 = x_2$, resp. $y_1 = y_2$. Uvědomte si přitom, že 0 a 1 neptří do nosiče operace. Neřešitelnost rovnice např. $2^x = 7$ v $\mathbb{N} \setminus \{1\}$ ukazuje, že operace není invertibilní.

10. Pouze operace uvedené v d) a f) jsou komutativní; aso-

ciativní jsou jen e) a f). Neřešitelnost rovnic $2^x = 5$ (pro b), $1 \circ x = 4$ (pro d), $4 \circ x = 5$ (pro e) a $y \circ 4 = 1$ (pro f) dokládá, že příslušné operace nejsou invertibilní. V c) má každá rovnice $a \circ x = 2a + x = c$ řešení $x = c - 2a$, zato $y \circ 2 = 2y + 2 = 3$ nemá řešení (v Z).
Pouze d) má neutrální prvek, a to 0.

11. Tabulkou operace je následující tabulka

	n	p	q	m
n	n	p	q	m
p	p	n	m	q
q	q	m	n	p
m	m	q	p	n

Uvedený součin je roven p. Soustava rovnic má řešení $x = n$, $y = p$. Neobyčejné zjednodušení rovnic a rovností dostaneme ze vztahů $p^2 = q^2 = m^2 = n$, kde n je neutrální prvek.

12. Řešení je $\mathbf{X} = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$. Při řešení je třeba využít toho, že násobení matic je vzhledem ke sčítání distributivní. Všechny v úloze uvedené matice jsou regulární.

Kapitola 4

1. Multiplikativní grupa nesoudělných zbytkových tříd modulo 12: p, p, p, p,;
množina všech reálných funkcí vzhledem ke sčítání: p, p, p, p;
množina $\{1, 2, 3, 6\}$ s operací $\wedge$: p, p, p, n.

2. Objekty a, b, c, d jsou pologrupy; e, f, g jsou komutativní grupy; h je grupa (ačkoli násobení matic není obecně komutativní, ukazuje se, že h je komutativní grupa).

3. a) Tabulka nepopisuje grupu, neboť operace není asociativní; je např. $(ab)d = cd = a$, ale $a(bd) = ac = d$.

b)

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

c) Vyznačené řádky, resp. sloupce nechť „přísluší" prvkům x a y, resp. z a u. Pak je $xz = e$, tj. $z = x^{-1}$, a $xu = a$, $yz = b$, Pro hledaný součin dostaneme $yu = yeu = yx^{-1}xu = (yx^{-1})(xu) = (yz)(xu) = ba$.

4. Objekty c, e, f jsou okruhy; d je těleso; a je okruh, jestliže prvky matic jsou racionální nebo reálná čísla (obecněji: jestliže jsou prvky nějakého tělesa); b není ani okruh, ani těleso.

5. a) Podle V(4.3) je třeba ještě ukázat invertibilitu operace. Rovnice $ax = b$ je vždy řešitelná, protože necháme-li x probíhat všech n prvků M (M je podle předpokladu konečná, má tedy n prvků), dostaneme n součinů $ax \in M$, mezi nimiž nemohou být dva stejné. Z $ax_1 = ax_2$ totiž plyne podle vlastnosti krácení $x_1 = x_2$. Dostaneme tedy pro n možných činitelů x právě n navzájem různých součinů ax z M, to ale znamená, že každý prvek z M (řekněme b) dostaneme jako nějaký součin ax_0. x_0 je tedy řešením rovnice $ax = b$. Analogicky se ukáže, že i rovnice $ya = b$ je vždy řešitelná.

b) Je-li $a \in U$ ($U \neq \emptyset$!), je podle definice podgrupy také $a^{-1} \in U$, a tudíž $a.a^{-1} = e \in U$. e neovlivňuje žádný prvek z G, a tím spíš ani z U. Je tedy e neutrální prvek U, a protože U je grupa, nemůže v U žádný jiný neutrální prvek existovat.

c) Je-li např. G podgrupa všech celých čísel dělitelných

dvěma (v aditivní grupě celých čísel) a H podgrupa všech celých čísel dělitelných třemi, je $4 \in G \cup H$ (neboť $4 \in G$) i $9 \in G \cup H$ (neboť $9 \in H$), ale $4 + 9 = 13 \notin G \cup H$, neboť je $13 \notin G$ i $13 \notin H$. Není tedy $G \cup H$ podgrupa.

d) Rovnice $ab + x = 0$ má podle definice inverzního prvku řešení $-(ab)$. Další řešení je $(-a)b$, jak ukazuje zkouška: $ab + (-a)b = (a + (-a))b = 0.b = 0$, přičemž jsme postupně použili distributivní zákon, definici inverzního prvku a úlohu nulového prvku při násobení. Protože ale rovnice $ab + x = 0$ je v okruhu řešitelná jednoznačně, platí tedy $-(ab) = (-a)b$. Analogicky se dokážou ostatní tvrzení.

e) Dostaneme ji přímým roznásobením na základě distributivního zákona; protože násobení v tělese je komutativní, můžeme jako obvykle místo $ab + ba$ psát $2ab$ (což by v případě $ab \neq ba$ nebylo možné).

6.

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

+	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

.	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

7. c) je homomorfismus, ale ostatní zobrazení jsou izomorfismy.

8. a) Izomorfii zjistíme porovnáním tabulek obou grup; izomorfní zobrazení φ je dáno vztahy $\varphi(f_1) = (1)_8$, $\varphi(f_2) = (3)_8$, $\varphi(f_3) = (5)_8$, $\varphi(f_4) = (7)_8$.

b) Označíme-li oba prvky $(H, +)$ jako 0 a a, bude zobrazení φ,

$$\varphi(g) = \begin{cases} 0, \text{ je-li } g \text{ sudé}, \\ a, \text{ je-li } g \text{ liché}, \end{cases}$$

homomorfismus $(Z, +)$ na $(H, +)$.

c) Aditivní grupa zbytkových tříd modulo 6 je izomorfní s multiplikativní grupou nesoudělných zbytkových tříd modulo 7 díky zobrazení φ, kde $\varphi((0)_6) = (1)_7$,

$\varphi((1)_6) = (3)_7$, $\varphi((2)_6) = (2)_7$, $\varphi((3)_6) = (6)_7$, $\varphi((4)_6) = (4)_7$, $\varphi((5)_6) = (5)_7$.

Aditivní grupa zbytkových tříd modulo 6 je izomorfní s multiplikativní grupou nesoudělných zbytkových tříd modulo 9 díky zobrazení η, kde $\eta((0)_6) = (1)_9$, $\eta((1)_6) = (2)_9$, $\eta((2)_6) = (4)_9$, $\eta((3)_6) = (8)_9$, $\eta((4)_6) = (7)_9$, $\eta((5)_6) = (5)_9$. Odtud dostaneme izomorfii grup nesoudělných zbytkových tříd modulo 7 a modulo 9 díky zobrazení $\varphi^{-1}\eta$. Protože aditivní grupa zbytkových tříd modulo 6 je cyklická, jsou cyklické i obě další grupy; jejich vytvořující prvky jsou $(3)_7$, resp. $(2)_9$.

d) Především je φ vzájemně jednoznačné zobrazení G na G. Aby φ byl izomorfismus, musí platit: $\varphi(ab) = \varphi(a)\varphi(b)$, to ale znamená, že $(ab)^{-1} = a^{-1}b^{-1}$. Obecně v každé grupě platí $(ab)^{-1} = b^{-1}a^{-1}$. Je tedy φ izomorfismus, právě když G jekomutativní.

9. a) $U_1 = \{1\}$, $U_2 = \{1; 4\}$, $U_3 = \{1; 11\}$, $U_4 = \{1; 14\}$, $U_5 = \{1, 2, 4, 8\}$, $U_6 = \{1, 4, 7, 13\}$.

b) Řád 12: $\{a^0, a^1, \ldots, a^{11}\} = \langle a\rangle$,
řád 6: $\{a^0, a^2, a^4, a^6, a^8, a^{10}\} = \langle a^2\rangle = \langle a^{10}\rangle$,
řád 4: $\{a^0, a^3, a^6, a^9\} = \langle a^3\rangle = \langle a^9\rangle$,
řád 3: $\{a^0, a^4, a^8\} = \langle a^4\rangle = \langle a^8\rangle$,
řád 2: $\{a^0, a^6\} = \langle a^6\rangle$,
řád 1: $\{a^0\} = \langle a^0\rangle$.

c) Každý homomorfní obraz grupy sestává z úplných obrazů při odpovídajícím homomorfním zobrazení, tedy podle cvičení 9a:
$G/U_1 = G$, $G/U_2 = \{\{1; 4\}, \{2; 8\}, \{7; 13\}, \{11; 14\}\}$,
$G/U_3 = \{\{1; 11\}, \{2; 7\}, \{4; 14\}, \{8; 13\}\}$,
$G/U_4 = \{\{1; 14\}, \{2; 13\}, \{4; 11\}, \{7; 8\}\}$,
$G/U_5 = \{\{1, 2, 4, 8\}, \{7, 11, 13, 14\}\}$,
$G/U_6 = \{\{1, 4, 7, 13\}, \{2, 8, 11, 14\}\}$.

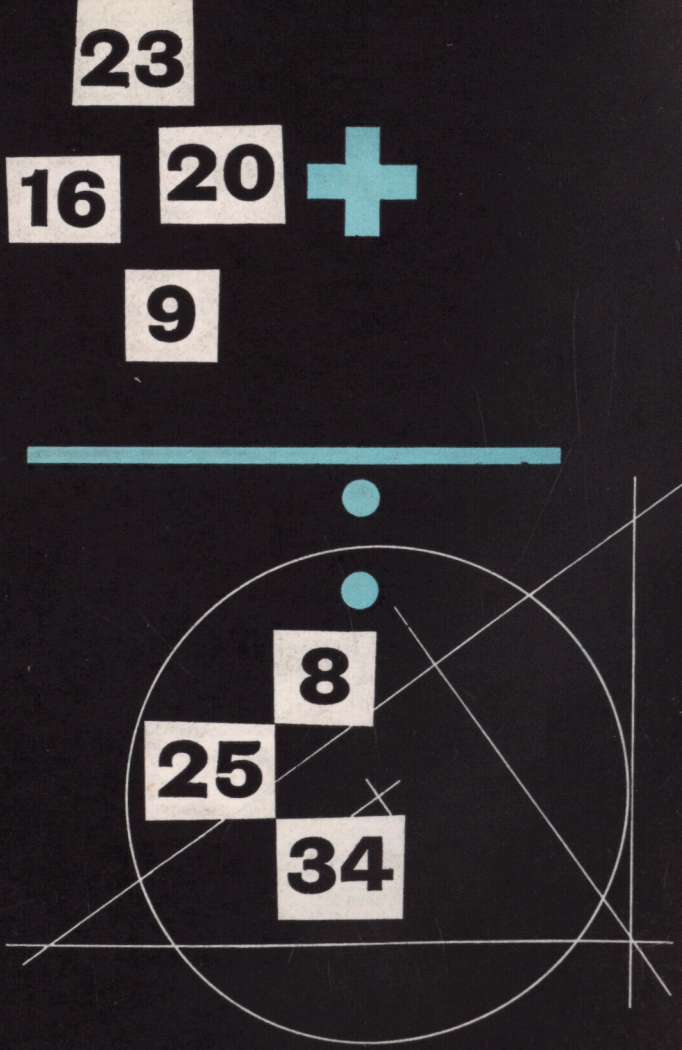
OBSAH

ŠKOLA MLADÝCH MATEMATIKŮ

HERBERT KÄSTNER, PETER GÖTHNER

ALGEBRA
Každý začátek je lehký

Pro účastníky matematické olympiády
vydává ÚV matematické olympiády
v nakladatelství Mladá fronta
Řídí akademik Josef Novák
Z německého originálu Algebra - aller Anfang ist leicht
přeložil Karel Horák
Obálku navrhl Jaroslav Příbramský
K tisku připravil Vladimír Doležal
Technický redaktor Vladimír Vácha
Odpovědná redaktorka Zdena Šmídová
Publikace číslo 4821
Edice Škola mladých matematiků, svazek 58
Vytiskl Mír, novinářské závody, n. p.
závod 1, Praha 1, Václavské nám. 15
7,95 AA, 8,61 VA, 1. vydání, 176 stran.
Náklad 9000 výtisků. Praha 1986. 508/21/82.5
23-080-86 03/2 Cena brož. výtisku 10 Kčs



23 - 080 - 86
03/2
Cena brož.
10 Kčs