ÚVOD

Pětisemestrová přednáška "Algebra a teoretická aritmetika" je základní algebraickou přednáškou pro posluchače učitelského studia s matematikou, která má významné postavení v celkové koncepci přípravy budoucích učitelů matematiky. Tato skripta jsou prvním dílem učebního textu k této přednášce a pokrývají zhruba látku probíranou v ní v 1. a 2. semestru.

Skripta jsou napsána tak, aby obsah, forma a pokud možno i sled jednotlivých částí co nejpřesněji odpovídaly platným osnovám. Výklad je při tom veden se snahou, aby v rámci daných možností byl co nejnázornější a pokud možno co nejpochopitelnější i těm čtenářům, jejichž dosavadní matematické znalosti a představy nejsou zrovna nejlepší. Na druhé straně však zdůrazněme, že pojmy, s nimiž se v textu pracuje, jsou svou logickou stavbou poměrně jednoduché a posluchačům zčásti známé ze střední školy, takže jsou přímo předurčeny k uvedení do vysokoškolského studia matematiky a k rozvíjení vhodných matematických návyků. Získaných poznatků se pak bezprostředně využívá v dalších matematických disciplinách (především v geometrii) a při aplikacích v řadě jiných oborů. Netřeba snad zvlášť zdůrazňovat, že algebra není pouze teoretickou matematickou disciplinou, ale že typická je její aplikovatelnost a široké použití v každodenní praxi (např. mezi nejčastěji řešené úlohy v každém odvětví průmyslu nebo zemědělství patří maticové úlohy nebo úlohy vedoucí na řešení soustav lineárních rovnic, atd.)

Po formální stránce je látka probíraná co nejpodrobněji, přičemž se vždy výslovně připomínají drobná úskalí a důležité maličkosti, které by méně zkušený čtenář často přehlédl. Z těchto důvodů má podrobné studium poznámek a komentářů přinejmenším stejný význam jak "učení se" definic a vět. Totéž platí i pro důkazy jednotlivých tvrzení, které jsou zde (na rozdíl od některých jiných disciplin) v převážné většině naprosto přirozené, průzračné a bez umělých obratů. Z metodických důvodů jsou důkazy tvrzení buď řádně provedeny nebo je uveden přesný odkaz. Občasné výzvy k samostatnému provedení, resp. ověření drobných maličkostí mají také svůj smysl a čtenář

by se rozhodně měl o ně pokusit. Většina zaváděných pojmů je ilustrována na příkladech (volených obvykle záměrně tak, aby k nim nebyly nutné žádné další matematické znalosti), přičemž jsou uváděny i příklady negativní.

Ve skriptech je užívána běžná symbolika, většinou známá ze střední školy. Nově zaváděná označení jsou pak řádně vysvětlena v textu. Důkazy jednotlivých tvrzení a řešení příkladů jsou opticky odděleny od ostatního textu uzavřením do hranatých závorek. Pro označování základních číslených množin je použito těchto standartních symbolů:

N . . . množina všech přirozených čísel
Z . . . množina všech celých čísel
Q . . . množina všech racionálních čísel
R . . . množina všech reálných čísel
K . . . množina všech komplexních čísel

Na konci textu uvedený seznam literatury je pouze velmi stručným výčtem několika dostupných titulů. Z nich připomeňme především světoznámou sovětskou Kurošovu učebnici [6], která dnes již v jedenácti vydáních a ve stotisícových nákladech je základní vysokoškolskou učebnicí algebry po více než 35 let. V seznamu uvedené sbírky úloh [8] - [12] pak obsahují dostatečné množství různě obtížných příkladů k procvičení probírané látky.

I. OPAKOVÁNÍ A DOPLNĚNÍ STŘEDOŠKOLSKÉ LÁTKY

§ 1. Základní logické pojmy.

V matematice se zabýváme studiem vlastností různých objektů a vztahů mezi nimi. K označování matematických objektů užíváme různých symbolů. Některé z nich mají pevný význam a nazýváme je **konstanty** (například symboly 1, π, $\sqrt{2}$, atd.); jiné takový přesně stanovený význam nemají, ale můžeme za ně konstanty vhodným způsobem dosazovat a nazýváme je **proměnné.** U proměnných musí být vždy vymezena množina těch objektů, jejichž symboly můžeme za proměnné dosazovat (například *"přirozené číslo x"*, *"přímka p"*, atd.).

Výrok je sdělení, o němž má smysl říci, že je pravdivé nebo nepravdivé. Hovoříme pak o pravdivém výroku, resp. nepravdivém výroku. Například sdělení *"Praha je hlavním městem ČSSR"* je pravdivým výrokem, resp. sdělení *"číslo sedm je sudé"* je nepravdivým výrokem. Může se však stát, že dané sdělení je výrokem, o němž však momentálně neumíme rozhodnout, zdali pravdivým či nepravdivým. Takovým je například výrok *"Mimo naši sluneční soustavu žijí myslící bytosti"*.

Každému výroku V se přiřazuje jeho **pravdivostní hodnota** $p(V)$ takto: je-li výrok V pravdivý, klademe $p(V) = 1$; je-li výrok V nepravdivý, klademe $p(V) = 0$.

Logické spojky nám umožňují z jednotlivých výroků tvořit další, složitější výroky. Nejběžněji se používá pět následujících logických spojek, které mají své ustálené názvy i označení, jak je přehledně uvedeno v následující tabulce (kde A, B značí libovolné výroky):

Název logické spojky	Označení	Slovní vyjádření
negace	$\neg A$	není pravda, že A
konjunkce	$A \wedge B$	A a (současně) B
disjunkce	$A \vee B$	A nebo B
implikace	$A \Rightarrow B$	jestliže A, pak B
ekvivalence	$A \Leftrightarrow B$	A právě když B

Každou z uvedených logických spojek popíšeme nyní tak, že uvedeme, jaké pravdivostní hodnoty přiřazujeme výroku, utvořenému s její pomocí (a to v závislosti na pravdivostních hodnotách výchozích výroků). Vznikne tak tzv. **tabulka pravdivostních hodnot**, která má pro negaci dva řádky a pro ostatní logické spojky čtyři řádky.

$p(A)$	$p(\neg A)$
1	0
0	1

$p(A)$	$p(B)$	$p(A \wedge B)$	$p(A \vee B)$	$p(A \Rightarrow B)$	$p(A \Leftrightarrow B)$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Tabulka 1

Rozeberme si nyní podrobněji jednotlivé logické spojky.

Negace libovolného výroku A se dá vždy bez problémů správně utvořit obratem "není pravda, že A". Tato formulace bývá však jazykově poněkud kostrbatá, a proto se snažíme i v matematice tvořit negace výroků bez užití tohoto obratu. Například místo *"není pravda, že číslo 7 je dělitelné třemi"* řekneme jistě raději *"číslo 7 není dělitelné třemi"*, atd.

Konjunkce výroků působí obvykle nejméně potíží. Z tabulky vidíme, že výrok $A \wedge B$ je pravdivý jedině v případě, že oba výroky A, B jsou pravdivé.

Disjunkce $A \vee B$ je pravdivá, je-li pravdivý alespoň jeden z výroků A, B (to jest jeden, resp. druhý, resp. oba dva). Zde tedy při použití spojky "nebo" dochází k odchylce od běžné hovorové řeči, v níž se spojka "nebo" téměř vždy používá ve smyslu vylučovacím (*"Přijedu v sobotu nebo v neděli"*, atd.).

Implikace $A \Rightarrow B$ je nepravdivá pouze v jediném případě, a sice, když výrok A je pravdivý a výrok B je nepravdivý. Ve všech ostatních případech je implikace pravdivá. Zejména je nutné si uvědomit, že implikace $A \Rightarrow B$ je vždy pravdivá v případě, že výrok A je nepravdivý (a to bez ohledu na to, jak vypadá výrok B).

Ekvivalence $A \Leftrightarrow B$ je pravdivá v případě, že oba výroky A, B jsou současně pravdivé nebo současně nepravdivé. Výroky A, B pak nazýváme též ekvivalentními výroky.

Velká část matematických úvah představuje vlastně tvoření a zápis ekvivalencí. Z častěji používaných připomeňme následující dvě, které ukazují, jak je možné vyjádřit negaci konjunkce a negaci disjunkce dvou výroků A, B:

$$\neg(A \wedge B) \quad \Leftrightarrow \quad \neg A \vee \neg B$$

$$\neg(A \vee B) \quad \Leftrightarrow \quad \neg A \wedge \neg B$$

O správnosti obou tvrzení se můžeme přesvědčit z následující tabulky pravdivostních hodnot:

$p(A)$	$p(B)$	$p(\neg A)$	$p(\neg B)$	$p(\neg(A \wedge B))$	$p(\neg A \vee \neg B)$	$p(\neg(A \vee B))$	$p(\neg A \wedge \neg B)$
1	1	0	0	0	0	0	0
1	0	0	1	1	1	0	0
0	1	1	0	1	1	0	0
0	0	1	1	1	1	1	1

Tabulka 2.

Podobným způsobem (viz tabulka 3) lze ukázat, že například:

(1) $A \Leftrightarrow B \quad \Leftrightarrow \quad (A \Rightarrow B) \wedge (B \Rightarrow A)$

(2) $A \Rightarrow B \quad \Leftrightarrow \quad \neg B \Rightarrow \neg A$

tj. ekvivalenci je možno vyjádřit pomocí konjunkce dvou implikací; resp. implikace $A \Rightarrow B$ je ekvivalentní implikaci $\neg B \Rightarrow \neg A$.

$p(A)$	$p(B)$	$p(\neg A)$	$p(\neg B)$	$p(A \Rightarrow B)$	$p(\neg B \Rightarrow \neg A)$	$p(B \Rightarrow A)$	$p(A \Leftrightarrow B)$	$p((A \Rightarrow B) \wedge (B \Rightarrow A))$
1	1	0	0	1	1	1	1	1
1	0	0	1	0	0	1	0	0
0	1	1	0	1	1	0	0	0
0	0	1	1	1	1	1	1	1

Tabulka 3.

Všimněme si, že sdělení obsahující nějakou proměnnou, například *"celé číslo x je větší než 1"*, není výrokem. Z tohoto sdělení se stane výrok (ať už pravdivý nebo nepravdivý) teprve tehdy, až za proměnnou x dosadíme nějakou konstantu z příslušné množiny, z níž můžeme konstanty volit, v našem případě tedy některé konkretní celé číslo. Při tom je zřejmé, že takovéto sdělení může obsahovat případně i více proměnných (například *"reálné číslo x je menší než reálné číslo y"* obsahuje dvě proměnné x, y atd.). Sdělení obsahující proměnné, z něhož se stane výrok teprve po dosazení (přípustných) konstant na místo proměnných, se nazývá **výroková funkce** (nebo též **výroková forma**). Je-li $V(x_1, \ldots, x_n)$ výroková funkce obsahující proměnné $x_1, \ldots, x_n$, pak její **definiční obor** (pokud není vymezen jiným způsobem), je množina všech n-tic $(a_1, \ldots, a_n)$ takových, že $V(a_1, \ldots, a_n)$ je výrok. **Obor pravdivosti** výrokové funkce $V(x_1, \ldots, x_n)$ je pak množina těch n-tic z definičního oboru, po jejichž dosazení za proměnné obdržíme pravdivý výrok.

Z výrokové funkce můžeme tedy utvořit výrok tím, že za všechny proměnné dosadíme konstanty z definičního oboru této výrokové funkce. Stejně častá a obvyklá je však i jiná

možnost, tzv. **kvantifikace proměnných**, jejíž pomocí utvoříme z výrokové funkce tzv. **kvantifikovaný výrok**. Spočívá v tom, že nějak udáme počet objektů, pro něž z výrokové funkce obdržíme pravdivý výrok. Ta část výroku, v níž je tento počet udáván, se nazývá **kvantifikátor**. Příkladem kvantifikátoru jsou vazby: *"každý"*, *"právě jeden"*, *"alespoň jeden"*, *"nejvýše jeden"*, *"právě čtyři"*, atd. K tomu poznamenejme, že zejména při používání obratů *"alespoň jeden"* a *"nejvýše jeden"*, které jsou v matematice velmi časté, je nutné si vždy uvědomovat jejich plný význam (tj. *"alespoň jeden"* znamená totéž co *"existuje"*, resp. *"jeden nebo více"*; podobně *"nejvýše jeden"* znamená *"žádný anebo jeden"*.) Tedy například z výše uvedené výrokové funkce *"celé číslo x je větší než 1"* je možné utvořit třeba tyto kvantifikované výroky:

"každé celé číslo x je větší než 1" (nepravdivý výrok)
"právě jedno celé číslo x je větší než 1" (nepravdivý výrok)
"alespoň jedno celé číslo x je větší než 1" (pravdivý výrok)
"nejvýše jedno celé číslo x je větší než 1" (nepravdivý výrok). atd.

Nejběžněji používanými jsou následující dva kvantifikátory, které mají i své ustálené názvy a označení:

a) **obecný kvantifikátor**, který vyjadřujeme slovy *"pro každý prvek (z definičního oboru výrokové funkce nebo jeho části) platí ..."* a označujeme symbolem $\forall$.
b) **existenční kvantifikátor**, který vyjadřujeme slovy *"existuje (alespoň jeden) prvek (z definičního oboru výrokové funkce), pro který platí ..."* a označujeme symbolem $\exists$.

V matematických uvahách je třeba velmi často provádět negace kvantifikovaných výroků. Jak již bylo řečeno dříve, nepoužíváme ani zde gramaticky kostrbatého obratu *"není pravda, že ..."*. Ukažme si nyní schematicky princip tvoření negace výroku s obecným, resp. s existenčním kvantifikátorem, s nimiž se v praxi nejčastěji setkáváme:

a) výrok s obecným kvantifikátorem tvaru:
"pro každý prvek z oboru U platí W"
a jeho negace
"existuje prvek z oboru U, pro který neplatí W"
b) výrok s existenčním kvantifikátorem tvaru:
"existuje prvek z oboru U, pro který platí W"
a jeho negace
"pro každý prvek z oboru U neplatí W",
přičemž v posledním případě je možné podle okolností slovo *"každý"* nahradit někdy

gramaticky vhodnějším slovem *"žádný"*. K tomu ještě poznamenejme, že při tvoření kvantifikovaných výroků a jejich negací můžeme samozřejmě užít i jiných gramatických obratů, které však musí zachovávat daný smysl. Ukažme si to na následujícím příkladu. Mějme dán kvantifikovaný výrok:

"každé auto na tomto parkovišti je červené"

který můžeme přeformulovat například do tvaru:

"všechna auta na tomto parkovišti jsou červená".

Negací tohoto kvantifikovaného výroku je pak výrok:

"existuje auto na tomto parkovišti, které není červené"

který můžeme případně přeformulovat do tvaru:

"alespoň jedno auto na tomto parkovišti není červené".

Upozorněme v této souvislosti velmi důrazně na to, že negací výroku *"každé auto na tomto parkovišti je červené"* není výrok *"žádné auto na tomto parkovišti není červené"* ani výrok *"alespoň jedno auto na tomto parkovišti je modré"*, atd.

Na závěr tohoto paragrafu si ještě stručně všimneme struktury matematických vět (tvrzení) a jejich důkazů. Této problematice je nutné důkladně porozumět a při dalším studiu tohoto textu (kde půjde vlastně o aplikace níže uvedených obecných zásad) se k ní případně vracet.

Matematické věty mají nejčastěji tvar implikace výroků nebo ekvivalence výroků.

Je-li **matematická věta tvaru implikace výroků** $P \Rightarrow T$, pak se výrok P nazývá předpokladem věty a výrok T tvrzením věty. Je-li implikace $P \Rightarrow T$ pravdivá, pak říkáme též, že P je **postačující** (nebo též **dostatečná) podmínka** pro T, resp., že T je **nutná podmínka** pro P.

K důkazu matematických vět tvaru implikace $P \Rightarrow T$ užíváme obvykle

a) **důkaz přímý**, který spočívá v tom, že z platnosti předpokladu P řadou platných implikací odvodíme platnost tvrzení T, tzn. hledáme výroky $A_1, \ldots, A_n$ tak, že platí: $P \Rightarrow A_1 \; ; \; A_1 \Rightarrow A_2 \; , \ldots \ldots , A_{n-1} \Rightarrow A_n \; ; A_n \Rightarrow T$

b) **důkaz nepřímý** spočívá v přímém důkazu věty $\neg T \Rightarrow \neg P$ (uvědomme si, že podle (2) platí $P \Rightarrow T$ právě když platí $\neg T \Rightarrow \neg P$ a z logického hlediska je tedy jedno, platnost které z obou uvedených implikací dokazujeme). Předpokládáme tedy, že je pravdivý výrok $\neg T$ (jinak řečeno, není pravdivé tvrzení T) a řadou platných implikací dokážeme, že pak není pravdivý předpoklad P.

Určitou modifikací nepřímého důkazu je tzv. **důkaz sporem**, kdy předpokládáme plat-

nost P a $\neg T$ a řadou platných implikací pak odvodíme spor s některým z předpokladů nebo s jiným výrokem (sporem rozumíme situaci, kdy nějaký výrok a jeho negace mají být současně pravdivé - je zřejmé, že tato situace nemůže nastat). Znamená to tedy, že musí platit T.

Matematická věta tvaru ekvivalence $A \Leftrightarrow B$ se dokazuje většinou tak, že dokážeme zvlášť platnost implikace $A \Rightarrow B$ a implikace $B \Rightarrow A$ (a to metodami popsanými výše). Uvědomme si, že správnost této úvahy vyplývá z (1), kde jsme ukázali, že $A \Leftrightarrow B$ je ekvivalentní s konjunkcí $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Někdy mívají matematické věty také tvar: "*jestliže platí výrok* P, *pak výroky* $A_1, \ldots, A_n$ $(n \geqslant 2)$ *jsou ekvivalentní*". (Poznamenejme, že pojem ekvivalentních výroků, který jsme zavedli pro dva výroky, můžeme lehce rozšířit na libovolný konečný počet výroků $A_1, \ldots, A_n$ $(n \geqslant 2)$ takto: řekneme, že výroky $A_1, \ldots, A_n$ jsou ekvivalentní, jestliže platí $A_i \Leftrightarrow A_j$, pro každé $i, j = 1, \ldots, n$). Věta tohoto tvaru se většinou dokazuje tak, že za předpokladu platnosti výroku P dokážeme platnost implikací:

(3) $$A_1 \Rightarrow A_2,\ A_2 \Rightarrow A_3, \ldots\ldots, A_{n-1} \Rightarrow A_n,\ A_n \Rightarrow A_1 .$$

Uvědomme si, že odsud již okamžitě vyplývá ekvivalentnost výroků $A_1, \ldots, A_n$. Bylo by samozřejmě také možné při důkazu postupovat přímo podle definice ekvivalentních výroků a za předpokladu platnosti P dokazovat všechny ekvivalence $A_i \Leftrightarrow A_j$ (zřejmě pro $i \neq j$). Tento postup by však byl jistě zdlouhavější. Konečně poznamenejme, že pořadí výroků $A_1, \ldots, A_n$ ve (3) zřejmě není podstatné; bylo by jistě možné vyjít od libovolného z výroků $A_1, \ldots, A_n$ a dokazovat n implikací tvaru

$$\ldots, A_i \Rightarrow A_j,\ A_j \Rightarrow A_k, \ldots$$

v nichž se každý z výroků $A_1, \ldots, A_n$ objeví právě jedenkrát jako předpoklad a jedenkrát jako tvrzení. Nepřesně, ale názorně řečeno - je pouze nutné, aby se nám "kruh implikací uzavřel".

Zvláštním typem důkazu matematické věty je **důkaz matematickou indukcí**. Matematickou indukcí není možné dokazovat jakoukoliv matematickou větu, nýbrž jenom ty věty, které tvrdí, že za určitých předpokladů platí výrok $V(n)$, pro všechna celá čísla $n \geqslant n_0$, kde n_0 je nějaké pevné celé číslo (nejčastěji je $n_0 = 1$). Důkaz matematickou indukcí pak probíhá ve dvou krocích: za daných předpokladů

α) dokážeme platnost výroku $V(n_0)$

β) předpokládáme, že výrok $V(n)$ platí pro $n = n_0, n_0 + 1, \ldots, k$ a za tohoto předpokladu dokážeme platnost výroku $V(k + 1)$. Věta je pak dokázána.

Předpoklad provedený v β) se nazývá indukční předpoklad. Poznamenejme, že ve velké většině důkazů matematickou indukcí se z indukčního předpokladu využije pouze to, že platí $V(k)$ a z platnosti $V(k)$ se již odvodí platnost $V(k + 1)$. Mohlo by se tedy zdát, že stačí indukční předpoklad "redukovat" na předpoklad platnosti $V(k)$. V dalším však budeme provádět několik důkazů matematickou indukcí, kde podobná "redukce" nebude možná. V těchto případech je potom nutné podle potřeby rozšířit krok α) o důkaz platnosti výroku $V(n_0 + 1)$, případně dalších (použijeme-li například z indukčního předpokladu platnost $V(k)$ a $V(k - 1)$, pak zřejmě musí být $k \geqslant n_0 + 1$, a tedy v kroku α) je nutné dokázat platnost $V(n_0)$ a $V(n_0 + 1)$).

§ 2. Základní množinové pojmy.

Se základními množinovými pojmy se na střední škole běžně a ve značném rozsahu pracuje. Nebudeme zde tedy opakovat podrobně vše, co by měl každý ze střední školy znát, ale připomeneme pouze ta základní fakta, která budou pro náš další výklad nezbytně nutná.

Symbol $x \in A$ čteme obvykle "x je prvkem (množiny) A" nebo "x patří do A" nebo "x leží v A". Z gramatických důvodů není vhodné používat slovní obrat "x (je) element A". Skutečnost, že prvek x nepatří do množiny A, budeme označovat symbolem $x \notin A$. Jestliže množiny A, B mají tytéž prvky, pak říkáme, že jsou si rovné a píšeme $A = B$.

Množiny můžeme popisovat různými způsoby - například výčtem prvků, pomocí pevně dohodnutých symbolů nebo jako obor pravdivosti určité výrokové funkce. Je-li tedy například $V(x)$ výroková funkce s definičním oborem D, pak

$$\{x \mid x \in D,\ V(x)\} \text{ nebo stručněji } \{x \in D \mid V(x)\}$$

značí obor pravdivosti této výrokové funkce, tj. množinu všech prvků $x \in A$, pro které platí $V(x)$. Konkretně třeba:

$$\{x \mid x \in N,\ 6 \leqslant x < 10\} = \{6, 7, 8, 9\}$$

$$\{x \mid x \in N,\ 6 < x < 6\} = \phi$$

kde symbol ϕ značí prázdnou množinu, tj. množinu, která neobsahuje žádný prvek (poznamenejme, že prázdná množina existuje jenom jedna).

Množina, která se skládá jen z konečného počtu prvků se nazývá **konečná množina**. Každá jiná množina se nazývá **nekonečná množina**. Připomeňme, že prázdnou množinu ϕ považujeme za konečnou množinu a říkáme, že počet prvků prázdné množiny je roven nule.

Řekneme, že množina A je **podmnožina** množiny B právě tehdy, jestliže každý prvek množiny A patří do množiny B. Píšeme pak $A \subseteq B$ (nebo též $B \supseteq A$). Jestliže $A \subseteq B$ a $A \neq B$, pak říkáme, že A je **vlastní podmnožina** množiny B a píšeme $A \subset B$ (nebo též $B \supset A$).

Vztahy $\subseteq$, $\supseteq$, $\subset$, $\supset$ mezi množinami se nazývají **množinové inkluse**. Množinovou inklusi $A \subseteq B$ obvykle dokazujeme přímo pomocí definice, tj. vezmeme libovolný prvek $x \in A$ a dokážeme, že $x \in B$. Připomeňme ještě, že jestliže množina A není podmnožinou množiny B, pak píšeme $A \not\subseteq B$. Chceme-li vztah $A \not\subseteq B$ dokázat, pak (podle úvah o negacích kvantifikovaných výroků) dokazujeme, že existuje prvek $x \in A$ takový, že $x \notin B$.

Jedním z nejčastěji prováděných důkazů v matematice vůbec je **důkaz rovnosti množin**, například $A = B$, který obvykle provádíme pomocí zřejmého tvrzení:

$$A = B \quad \text{právě když} \quad (A \subseteq B) \wedge (B \subseteq A)$$

tj. dokážeme nejdříve inklusi $A \subseteq B$ a pak inklusi $B \subseteq A$. Poznamenejme, že rovnost množin můžeme samozřejmě dokazovat i jinak, například logickým odvozením z definic nebo ze známých, dříve odvozených rovností množin, atd.

Poměrně často se v matematice setkáváme s množinami, jejichž prvky jsou zase množiny. Pro takovou množinu budeme užívat názvu **systém množin** (místo gramaticky neestetického názvu "množina množin"). Je nutné si na tento fakt zvyknout a naučit se zacházet se systémem množin stejně jako s každou jinou množinou.

Příklad 2.1.: Nechť A je libovolná množina. Pak všechny podmnožiny množiny A tvoří systém množin, který budeme nazývat **systém všech podmnožin množiny** A a označovat symbolem 2^A. Konkretně například pro $A = \{a, b, c\}$ je
$2^A = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ resp. pro $A = \phi$ je $2^A = \{\phi\}$, atd. Je-li množina A konečná, o n prvcích, pak množina 2^A je jistě také konečná a lze ukázat, že má 2^n prvků. Je-li A nekonečná, pak je množina 2^A zřejmě také nekonečná. Zkuste si například představit, jak vypadá množina 2^N.

Definice: Nechť $I \neq \phi$ je libovolná (tzv.indexová) množina. Nechť A_i je množina pro každé $i \in I$. Pak:
sjednocení množin A_i, $i \in I$ je množina

$$\bigcup_{i \in I} A_i = \{x \mid \exists i_0 \in I : x \in A_{i_0}\},$$

Průnik množin A_i, $i \in I$ je množina

$$\bigcap_{i \in I} A_i = \{x \mid \text{pro } \forall i \in I : x \in A_i\}.$$

Uvědomme si, že předchozí definice zahrnuje sjednocení a průnik jak konečného, tak i nekonečného počtu množin (záleží při tom zřejmě na indexové množině I). Sjednocení, resp. průnik konečného počtu množin $A_1, \ldots, A_n$ zapisujeme také často symbolem $A_1 \cup \ldots \cup A_n$, resp. $A_1 \cap \ldots \cap A_n$.

Jsou-li A, B dvě libovolné množiny, pak řekneme, že množiny A, B jsou **disjunktní**, je-li $A \cap B = \phi$, resp. řekneme, že A, B jsou **incidentní**, jestliže $A \cap B \neq \phi$.

Definice: Nechť A,B jsou množiny. **Rozdíl množin** A, B (v tomto pořadí) je pak množina

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Je-li navíc $B \subseteq A$, pak množina $A - B$ se nazývá **komplement** množiny B v množině A a označuje se symbolem B'_A nebo jen stručně B'.

Poznamenejme, že s komplementy pracujeme v matematice obvykle v situaci, kdy roli množiny A hraje jistá dostatečně velká, tzv. univerzální množina a všechny uvažované množiny jsou pak automaticky chápány jako podmnožiny v A. Tak například při úvahách o množinách čísel hraje roli množiny A obvykle množina všech komplexních čísel. Vznikne-li však nebezpečí nedorozumění, pak je vždy nutné množinu A přesně specifikovat.

Pro ilustraci základních množinových pojmů a práci s nimi se na střední škole často užívají tzv. **Vennovy diagramy**. Při konstrukci Vennova diagramu se do obdélníku představujícího jistou základní množinu (v níž se všechny úvahy odehrávají) zakreslují jednotlivé množiny pomocí vhodně volených čar, a to tak, aby vzniklá pole umožňovala vyšetřovat všechny možné případy vzájemné polohy daných množin (tj. při n výchozích množinách musíme dostat celkem 2^n polí). Je-li některá z množin prázdná, napíše se do příslušného pole symbol prázdné množiny. Prvek ležící v některé z množin se značí křížkem v příslušném poli. Na obr. 1a je nakreslen Vennův diagram pro dvě množiny A, B znázorňující, že $A \subset B$.

a) b)

Obr. 1

Pro lepší pochopení studovaných pojmů je dobré si občas kreslit jakési orientační náčrtky, zachycující podstatu dané situace. Obr. 1b) zachycuje tímto způsobem stejnou situaci jako Vennův diagram 1a), totiž, že $A \subset B$. Je samozřejmé, že tyto náčrtky v žádném případě nenahrazují důkazy tvrzení, ale pomáhají pouze názorné představě.

Pro sjednocení, průnik a rozdíl množin lze odvodit celou řadu tvrzení, z nichž si pro ilustraci uvedeme několik v následující větě.

Věta 2.1. *Nechť A, B, C jsou libovolné množiny; pak platí:*

1. $A \cup B = B \cup A$
2. $(A \cup B) \cup C = A \cup (B \cup C)$
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. $A - (B \cup C) = (A - B) \cap (A - C)$
6. $A - (B \cap C) = (A - B) \cup (A - C)$

1'. $A \cap B = B \cap A$

2'. $(A \cap B) \cap C = A \cap (B \cap C)$

[Důkaz všech tvrzení se provádí stejným způsobem (dokazováním množinových inklusí). Pro ilustraci si dokážeme například 6.:

"$\subseteq$": $x \in A - (B \cap C) \Rightarrow [x \in A \wedge x \notin (B \cap C)] \Rightarrow [x \in A \wedge (x \notin B \vee x \notin C)] \Rightarrow$

$\Rightarrow [x \in (A - B) \vee x \in (A - C)] \Rightarrow x \in (A - B) \cup (A - C)$

"$\supseteq$": $x \in (A - B) \cup (A - C) \Rightarrow [x \in (A - B) \vee x \in (A - C)] \Rightarrow [x \in A \wedge (x \notin B \vee x \notin C)] \Rightarrow$

$\Rightarrow [x \in A \wedge x \notin (B \cap C)] \Rightarrow x \in A - (B \cap C)$,

odkud pak dohromady dostáváme žádanou rovnost 6.].

Poznamenejme, že vztahy 1 a 1' (resp. 2 a 2', resp. 3 a 4, resp. 5 a 6) se nazývají

komutativní zákony (resp. asociativní zákony, resp. distributivní zákony, resp. de Morganova pravidla). Uvedená tvrzení lze zřejmým způsobem rozšířit na sjednocení a průniky systémů obsahujících případně i nekonečně mnoho množin.

Na závěr tohoto paragrafu si ještě zavedeme pojem kartézského součinu množin. K tomu však potřebujeme pojem **uspořádaná dvojice prvků**. Pro naše účely postačí intuitivní představa, že ke každým dvěma prvkům x, y lze přiřadit nový prvek (x, y), nazývaný uspořádanou dvojicí tak, že dvě uspořádané dvojice (x, y) a (x', y') jsou si rovny právě když $x = x'$ a $y = y'$. V uspořádané dvojici (x, y) tedy záleží na pořadí prvků x a y, přičemž prvek x nazýváme první složkou a prvek y nazýváme druhou složkou uspořádané dvojice (x, y).

Analogickým způsobem lze pro $n \geqslant 3$ zavést pojem uspořádané n-tice prvků, kterou označujeme symbolem $(a_1, \ldots, a_n)$. Při tom $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$ právě když $a_1 = b_1 \wedge \ldots \wedge a_n = b_n$, tzn. právě když se rovnají odpovídající si složky.

Definice: Nechť A, B jsou libovolné množiny. Pak množina

$$A \times B = \{(x, y) \mid x \in A, y \in B\}$$

se nazývá **kartézský součin** množin A, B (v tomto pořadí).

Z definice kartézského součinu je zřejmé, že množiny $A \times B$ a $B \times A$ jsou obecně různé. Je-li například $A = \{a\}$, $B = \{b_1, b_2\}$, pak

$$A \times B = \{(a, b_1), (a, b_2)\}, \text{ resp. } B \times A = \{(b_1, a), (b_2, a)\}$$

a tedy $A \times B \neq B \times A$.

Dále je zřejmé, že je-li některá z množin A, B prázdná, tzn. $A = \phi \vee B = \phi$, pak je i jejich kartézský součin prázdnou množinou, tzn. $A \times B = \phi$.

Analogickým způsobem zavádíme kartézský součin množin $A_1, \ldots, A_n$ $(n \geqslant 2)$ jako množinu

$$(1) \qquad A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i, i = 1, 2, \ldots, n\}$$

Je-li $A_1 = A_2 = \ldots = A_n = A$, značíme kartézský součin (1) symbolem A^n a nazýváme jej n-tá **kartézská mocnina** množiny A. Například tedy

$$R^3 = \{(x, y, z) \mid x, y, z \in R\}$$

je množinou všech uspořádaných trojic reálných čísel.

§ 3. Základní vlastnosti celých čísel

Na střední škole byla odvozena celá řada vlastností celých čísel a pravidel pro počítání s nimi. Víme, že ke každému celému číslu a se dá přiřadit jeho **absolutní hodnota** $|a|$, definovaná následovně:

$$|a| = \begin{cases} a & \text{je-li } a \geqslant 0 \\ -a & \text{je-li } a < 0 \end{cases}$$

Bezprostředně z této definice plyne, že pro každá dvě celá čísla a, b platí:

$$|a \,.\, b| = |a| \,.\, |b|$$
$$|a + b| \leqslant |a| + |b|$$

(dokažte si sami oba vztahy!). Dále si zopakujme základní vlastnosti dělitelnosti celých čísel.

Definice: Nechť a, b jsou celá čísla; řekneme, že a **dělí** b (označujeme $a \mid b$), jestliže existuje celé číslo z tak, že

$$b = a \,.\, z$$

V opačném případě říkáme, že a **nedělí** b (píšeme pak $a \nmid b$).

Poznamenejme, že místo obratu *"a dělí b"* můžeme použít též obratu *"b je dělitelné a"* nebo *"a je dělitelem b"*. Zvláštní roli při dělitelnosti celých čísel hraje číslo nula. Přímo z definice dělitelnosti totiž plyne, že $a \mid 0$ pro každé $a \in \boldsymbol{Z}$, tj. každé celé číslo dělí nulu a dále, že $0 \mid b$ právě když $b = 0$, tj. nula dělí pouze nulu.

Všimněme si dále, že každé celé číslo b je vždy dělitelné čísly $1, -1, b, -b$. Tato čísla se nazývají **nevlastní dělitelé** čísla b. Všichni ostatní dělitelé (pokud existují) se nazývají **vlastní dělitelé** čísla b. Přirozené číslo $p \geqslant 2$ se nazývá **prvočíslo**, (resp. **složené číslo**) jestliže má (resp. nemá) pouze nevlastní dělitele. Některé základní vlastnosti celých čísel, které souvisí s dělitelností, popisují následující věty.

Věta 3.1. *Nechť $a, b, c \in \boldsymbol{Z}$; pak platí:*

1. $a \mid a$
2. $a \mid b \wedge b \mid c \Rightarrow a \mid c$
3. $a \mid b \wedge a \mid c \Rightarrow a \mid (b \,.\, x + c \,.\, y)$ *pro každé* $x, y \in \boldsymbol{Z}$
4. $a \mid b \wedge b \neq 0 \Rightarrow |a| \leqslant |b|$

5. $a \mid b \wedge b \mid a \Leftrightarrow |a| = |b|$

6. *a je vlastním dělitelem* $b \Leftrightarrow a \mid b \wedge 1 < |a| < |b|$ *(pro* $b \neq 0$*)*

[D ů k a z: 1. zřejmé, neboť $a = a \,.\, 1$

2. zřejmé, neboť $b = a \,.\, z_1,\ c = b \,.\, z_2 \Rightarrow c = a \,.\, (z_1 \,.\, z_2)$

3. zřejmé, neboť $b = a \,.\, z_1,\ c = a \,.\, z_2 \Rightarrow bx + cy = a(z_1 x + z_2 y)$

4. $a \mid b \Rightarrow b = a \,.\, z\,;\ z \in \boldsymbol{Z},\ z \neq 0$. Přechodem k absolutním hodnotám dostaneme $|b| = |a| \,.\, |z|$, odkud plyne, že $|a| \leqslant |b|$.

5. "$\Rightarrow$" plyne ihned ze 4:

"$\Leftarrow$" $|a| = |b| \Rightarrow b = \pm a = a \,.\, (\pm 1) \wedge a = b \,.\, (\pm 1)$, odkud dostáváme, že $a \mid b \wedge b \mid a$

6. "$\Rightarrow$" dostaneme užitím 4.

"$\Leftarrow$" plyne přímo z definice vlastního dělitele]

Věta 3.2. (Věta o dělení se zbytkem celých čísel)

Nechť a, b jsou celá čísla, $b \neq 0$. Potom:
existují celá čísla q, r, splňující:

(1) $\qquad a = b \,.\, q + r\ ,\quad 0 \leqslant r < |b|\ ,$

přičemž vyjádření (1) je jednoznačné.

[D ů k a z věty provedeme ve dvou krocích:

I. důkaz existence vyjádření (1). Uvažme množinu

$$M = \{\, x \,.\, |b| \mid x \in \boldsymbol{Z} \wedge x \,.\, |b| \leqslant a \}$$

Zřejmě $M \neq \phi$ a v M existuje největší prvek, který označíme $x_0 \,.\, |b|$ (rozmyslete si podrobně, že tomu tak skutečně je!). Potom je:

(2) $\qquad a = x_0 \,.\, |b| + r, \qquad$ kde $r \geqslant 0$

a dále je $(x_0 + 1) \,.\, |b| > a$, tzn. $x_0 \,.\, |b| + |b| > a$, odkud dostáváme, že $a - x_0 \,.\, |b| < |b|$, neboli po dosazení ze (2):

(3) $\qquad r < |b|$

Nyní označme:

$$q = \begin{cases} x_0 & \text{je-li } b > 0 \\ -x_0 & \text{je-li } b < 0 \end{cases}$$

Při tomto označení dostáváme z (2) a (3) hledaný vztah (1).

II. důkaz jednoznačnosti vyjádření (1). Předpokládejme, že existují $q, q', r, r' \in \mathbf{Z}$, splňující:

$$a = b \,.\, q + r, \qquad 0 \leqslant r < |b|$$
$$a = b \,.\, q' + r', \qquad 0 \leqslant r' < |b| \,.$$

Pak odečtením obou rovnic dostaneme: $b(q - q') = r' - r$, odkud $|b \,.\, (q - q')| = |b| \,.\, |q - q'| = |r' - r|$. Dále, z předpokladu o r a r' plyne, že $|r' - r| < |b|$. Nyní - při $q \neq q'$ dostáváme: $|r' - r| = |b| \,.\, |q - q'| \geqslant |b|$, což je spor. Musí tedy být $q = q'$, odkud pak také $r = r'$, což znamená, že vyjádření (1) je jednoznačné.]

Číslo q (resp. r) z vyjádření (1) se nazývá **podíl** (resp. **zbytek**) po dělení čísla a číslem b. Vidíme tedy, že zbytek r po dělení čísla a číslem b je definován jednoznačně a nabývá právě jedné z hodnot $0, 1, \ldots, |b| - 1$. Uvědomme si, že věta o dělení se zbytkem není vlastně nic jiného, než přesně zformulovaný (a dokázaný) algoritmus pro dělení dvou celých čísel, používaný již na základní škole.

Definice: Nechť m je pevné přirozené číslo a nechť $a, b \in \mathbf{Z}$. Řekneme, že čísla a, b jsou **kongruentní podle modulu** m a píšeme $a \equiv b \pmod m$, jestliže $m \mid b - a$.

Věta 3.3. *Nechť m je pevné přirozené číslo a nechť $a, b \in \mathbf{Z}$. Pak následující výroky jsou ekvivalentní:*

(i) $a \equiv b \pmod m$

(ii) čísla a, b dávají po dělení číslem m stejný zbytek

(iii) čísla a, b se liší o celý násobek čísla m (tj. $\exists z \in \mathbf{Z}$ tak, že $b = a + z \,.\, m$).

[D ů k a z: "(i) ⇒ (ii)": nechť platí (i) a nechť $a = m \,.\, q_1 + r_1$, $b = m \,.\, q_2 + r_2$, kde $0 \leqslant r_1, r_2 < m$. Potom $r_2 - r_1 = (b - a) + m(q_1 - q_2)$. Ale $m \mid b - a$ (podle (i)) a triviálně $m \mid m$, tedy podle V.3.1.3. je $m \mid r_2 - r_1$. Zřejmě však $-m < r_2 - r_1 < m$, a tedy musí být $r_2 - r_1 = 0$, neboli $r_2 = r_1$. Platí tedy (ii).

"(ii) ⇒ (iii)": nechť platí (ii), tzn. $a = m \,.\, q_1 + r$, $b = m \,.\, q_2 + r$. Potom $r = a - mq_1 = b - mq_2$, odkud $b = a + (q_2 - q_1) \,.\, m$, kde zřejmě $(q_2 - q_1) \in \mathbf{Z}$. Platí tedy (iii).

"(iii) ⇒ (i)": nechť platí (iii), tzn. $b = a + z \,.\, m$, $z \in \mathbf{Z}$. Pak $b - a = z \,.\, m$, neboli $m \mid b - a$, tzn. platí (i).]

Definice: Nechť $a, b \in \mathbf{Z}$; pak číslo $d \in \mathbf{Z}$ se nazývá **největší společný dělitel** čísel a, b, platí-li:

(i) $d \mid a, \quad d \mid b$

(ii) jestliže $k \mid a, k \mid b$ pro nějaké $k \in \mathbf{Z}$, potom $k \mid d$.

Věta 3.4. *Nechť a, b jsou libovolná celá čísla. Pak platí:*

1. *existuje největší společný dělitel čísel a, b*
2. *je-li d největším společným dělitelem čísel a, b, pak $\{d, -d\}$ je množinou všech největších společných dělitelů čísel a, b*
3. *je-li d největším společným dělitelem čísel a, b, pak existují $u, v \in \mathbf{Z}$ tak, že*

$$a \cdot u + b \cdot v = d.$$

[Důkaz: 1. pro $a = 0, b = 0$ existuje největší společný dělitel, a sice číslo 0 (ověřte!). Nechť tedy $a \neq 0 \vee b \neq 0$. Uvažme množinu čísel

$$M = \{a.x + b.y \mid x, y \in \mathbf{Z} \text{ libovolné}\}$$

a označme $d = ax_0 + by_0$ nejmenší kladné číslo patřící do M (rozmyslete si, že takové číslo d určitě existuje!). Ukážeme, že d je největším společným dělitelem čísel a, b:

(i) podle V.3.2. existují $q, r \in \mathbf{Z}$ tak, že $a = d \cdot q + r$; $0 \leqslant r < d$ (zde $|d| = d$, protože d je kladné). Pak: $r = a - dq = a - (ax_0 + by_0) \cdot q = a \cdot (1 - x_0 q) + b(-y_0 q) \in M$. Poněvadž však d je nejmenším kladným číslem patřícím do M, musí být $r = 0$, což však znamená, že $a = d \cdot q$, a tedy $d \mid a$. Podobně se ukáže, že $d \mid b$.

(ii) jestliže $k \mid a, k \mid b$, pak podle V.3.1.3., $k \mid ax_0 + by_0 = d$.

Dohromady dostáváme, že d je největším společným dělitelem a, b.

2. plyne z definice největšího společného dělitele a z V 3.1.5.

3. z důkazu 1. části plyne, že existují $x_0, y_0 \in \mathbf{Z}$ tak, že $a \cdot x_0 + b \cdot y_0$ je největším společným dělitelem čísel a, b. Vzhledem k části 2. však libovolného z obou největších společných dělitelů čísel a, b vyjádříme ve tvaru $a \cdot (\pm x_0) + b \cdot (\pm y_0)$, odkud po vhodném označení dostáváme žádané tvrzení.]

Z předchozí věty plyne, že pro $a \neq 0 \vee b \neq 0$ existují vždy dva největší společní dělitelé čísel a, b, lišící se znaménkem. Kladný z těchto dvou největších společných dělitelů budeme označovat symbolem (a, b). Poznamenejme, že pro $a = b = 0$ existuje jediný jejich největší společný dělitel, a sice číslo 0. V tomto případě pak symbol (a, b) není definován. Dále - zřejmě platí $(x, 0) = (0, x) = |x|$, pro libovolné celé číslo $x \neq 0$.

Je-li $(a, b) = 1$, pak říkáme, že čísla a, b jsou **nesoudělná**. Jsou-li a, b nesoudělná, pak podle předchozí věty existují celá čísla u, v tak, že

$$a \,.\, u + b \,.\, v = 1 \,.$$

Na základě tohoto faktu lze dokázat celou řadu tvrzení o dělitelnosti čísel, běžně používaných na střední škole. Uveďme si alespoň některá z nich.

Věta 3.5. *Nechť* $a, b, c, a_1, \ldots, a_n \in \boldsymbol{Z}$; *pak platí:*

1. $(a, b) = 1 \wedge (a, c) = 1 \Rightarrow (a, b \,.\, c) = 1$
2. $a \mid b.c \wedge (a, b) = 1 \Rightarrow a \mid c$
3. p *je prvočíslo* $\wedge\ p \mid a_1 \,.\, \ldots \,.\, a_n \Rightarrow p \mid a_i$ *pro nějaké* $i = 1, 2, \ldots, n$.

[D ů k a z: 1. podle předchozí věty (část 3) existují celá čísla u, v, x, y tak, že $a \,.\, u + b \,.\, v = 1$, $a \,.\, x + c \,.\, y = 1$. Vynásobením obou rovností dostaneme:

(4) $$a \,.\, (uax + ucy + bvx) + bc \,.\, (vy) = 1$$

Nyní, z definice největšího společného dělitele již plyne, že $(a, bc) = 1$, neboť

(i) zřejmě $1 \mid a$, $1 \mid bc$

(ii) jestliže $k \mid a$, $k \mid bc$, pak ze (4) užitím V 3.1.3 dostáváme, že $k \mid 1$

2. podle předchozí věty (část 3) existují celá čísla u, v tak, že $a \,.\, u + b \,.\, v = 1$, odkud (po vynásobení číslem c) je: $acu + bcv = c$.

Odsud však podle V 3.1.3. dostáváme (poněvadž $a \mid a \wedge a \mid bc$), že $a \mid c$.

3. dokáže se matematickou indukcí vzhledem k n.

α) pro $n = 1$ tvrzení triviálně platí

β) předpokládáme, že tvrzení platí pro $1, \ldots, n$ $(n \geqslant 1)$ a dokážeme je pro $n + 1$. Nechť tedy $p \mid (a_1 \,.\, \ldots \,.\, a_n)\, a_{n+1}$. Pokud $p \mid a_{n+1}$, pak jsme hotovi. Nechť tedy $p \nmid a_{n+1}$. Pak je $(p, a_{n+1}) = 1$ a podle části 2. této věty je $p \mid a_1 \,.\, \ldots \,.\, a_n$. Podle indukčního předpokladu pak $p \mid a_i$ pro nějaké $i = 1, \ldots, n$.]

Věta 3.6. *Každé přirozené číslo* $a > 1$ *lze rozložit na součin prvočísel, a to až na jejich pořadí jednoznačně.*

[D ů k a z: I. existence rozkladu;

provedeme sporem. Předpokládejme, že existují přirozená čísla, která nelze rozložit na součin prvočísel a nejmenší z nich označme w. Pak ale w není prvočíslo, tzn. musí mít vlastního dělitele b, a tedy: $w = b \,.\, c$, kde $1 < b < w$, $1 < c < w$. Ale b i c lze rozložit na

součin prvočísel (jinak spor s minimalitou w), a tedy $w = b \cdot c$ má stejnou vlastnost; spor.

II. jednoznačnost rozkladu (až na pořadí); nechť

(5) $$a = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_s$$

jsou dva rozklady přirozeného čísla a na součin prvočísel. Jednoznačnost (až na pořadí činitelů) nyní dokážeme matematickou indukcí vzhledem k n.

α) pro $n = 1$ je a prvočíslem, tzn. musí být i $s = 1$

β) předpokládejme, že pro všechna přirozená čísla, mající alespoň jeden rozklad na součin méně než n prvočísel je tento rozklad jednoznačný (až na pořadí). Vezměme přirozené číslo a, pro něž platí (5). Potom $p_n \mid q_1 \cdot \ldots \cdot q_s$, tzn. podle V. 3.5.3. je $p_n \mid q_i$ pro nějaké $i = 1, \ldots, s$. Poněvadž jde o prvočísla, musí být $p_n = q_i$, takže po zkrácení číslem $p_n = q_i$ v (5) a užití indukčního předpokladu dostaneme žádanou jednoznačnost.]

Věta 3.7. *Prvočísel je nekonečně mnoho.*

[D ů k a z: provedeme sporem; předpokládejme, že existuje pouze konečně mnoho prvočísel, například $p_1, \ldots, p_n$. Číslo $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ lze podle předchozí věty rozložit na součin jistého počtu prvočísel, tzn. jinak řečeno, číslo a je dělitelné jistým počtem prvočísel. Ale a nemůže být dělitelné žádným z prvočísel p_i $(1 \leqslant i \leqslant n)$ (jinak, užitím V.3.1.3. dostaneme, že $p_i \mid 1$, spor), a tedy existuje alespoň jedno prvočíslo různé od $p_1, \ldots, p_n$; spor.]

§ 4. Relace

Pojem relace patří dnes v matematice mezi základní pojmy, s nimiž se studenti na střední škole setkávají velmi záhy.

Definice. Nechť A, B jsou libovolné množiny. Pak libovolná podmnožina ρ kartézského součinu $A \times B$ se nazývá **relace mezi množinami** A **a** B (v tomto pořadí). Je-li $(x, y) \in \rho$, pak říkáme, že prvek x je v relaci ρ s prvkem y. Naopak, jestliže $(x, y) \notin \rho$, pak říkáme, že prvek x není v relaci ρ s prvkem y.

Příklad 4.1.:

1. Nechť $A = \{a, b, c, d\}$, $B = \{x, y, z\}$; pak $\rho = \{(a, y), (c, y), (c, z)\}$ je relace mezi množinami A a B.

2. Nechť $A = N$, $B = N$; pak $\rho = \{(x, y) \in N \times N \mid y - x$ je kladné číslo$\}$ je rela-

ce mezi A a B. Je zřejmé, že v tomto případě je $(x, y) \in \rho$ právě tehdy když číslo x je menší než číslo y (při uspořádání čísel podle velikosti).

3. Nechť A, B jsou libovolné množiny;

a) zřejmě $\phi \subseteq A \times B$, a tedy $\rho = \phi$ je relace mezi A a B, která se nazývá **prázdná relace** mezi A a B. Je to tedy taková relace, kdy žádný prvek z A není v relaci s žádným prvkem z B.

b) druhým extrémem je relace $\rho = A \times B$, která se nazývá **univerzální relace** mezi A a B. Je to tedy relace mezi A a B taková, že každý prvek z A je v relaci s každým prvkem z B.

Při této příležitosti si ještě řekněme, že v definici relace mezi množinami A a B není vyloučen případ, že $A = \phi$ nebo $B = \phi$. V tomto případě je zřejmě $A \times B = \phi$ a tedy jedinou možnou relací mezi A a B je potom prázdná relace.

Vidíme tedy, že definovat relaci ρ mezi A a B znamená vlastně popsat jistou podmnožinu ρ v $A \times B$, tj. v podstatě jakýmkoliv korektním způsobem jednoznačně určit všechny uspořádané dvojice z $A \times B$, které patří do ρ.

Definice. Nechť ρ je relace mezi množinami A a B. Potom množina

$$\mathrm{Dom}\ \rho = \{x \in A \mid \exists y \in B \text{ tak, že } (x,y) \in \rho\}$$

se nazývá **definiční obor relace** ρ. Množina

$$\mathrm{Im}\ \rho = \{y \in B \mid \exists x \in A \text{ tak, že } (x,y) \in \rho\}$$

se nazývá **obraz relace** ρ.

Poznámka: označení Dom, resp. Im jsou v matematice běžně používané zkratky slov "domain", resp. "image", což jsou anglické ekvivalenty pro výrazy "definiční obor", resp. "obraz". Někdy se místo obratu definiční obor (resp. obraz) relace ρ používá též obratu první (resp. druhý) obor relace ρ.

Příklad 4.2. Definiční obory a obrazy relací z příkladu 4.1. jsou zřejmě:

1. $\mathrm{Dom}\ \rho = \{a, c\}$, $\mathrm{Im}\ \rho = \{y, z\}$
2. $\mathrm{Dom}\ \rho = N$, $\mathrm{Im}\ \rho = N - \{1\}$
3. pro prázdnou relaci ρ je $\mathrm{Dom}\ \rho = \phi$, $\mathrm{Im}\ \rho = \phi$
   pro univerzální relaci ρ je $\mathrm{Dom}\ \rho = A$, $\mathrm{Im}\ \rho = B$.

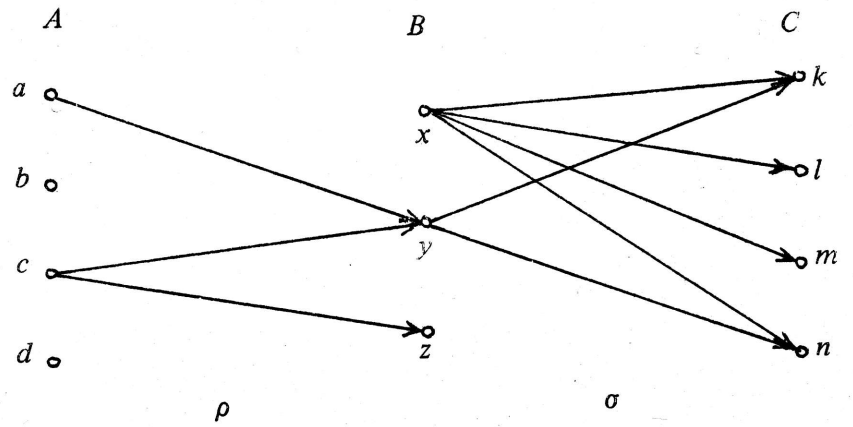
Definice. Nechť ρ je relace mezi množinami A a B; nechť σ je relace mezi množinami B a C. Pak relace

$$\sigma \circ \rho = \{(x, y) \in A \times C \mid \exists b \in B \text{ tak, že } (x, b) \in \rho \wedge (b, y) \in \sigma\}$$

se nazývá **složená relace** z relací ρ a σ. (symbol $\sigma \circ \rho$ čteme buď σ kolečko ρ nebo σ po ρ).

Příklad 4.3.: Nechť $A = \{a, b, c, d\}$, $B = \{x, y, z\}$, $C = \{k, l, m, n\}$; nechť $\rho = \{(a, y), (c, y), (c, z)\}$; $\sigma = \{(x, k), (x, l), (x, m), (x, n), (y, k), (y, n)\}$. Potom je $\sigma \circ \rho = \{(a, k), (a, n), (c, k), (c, n)\}$.

Poznámka: Pro větší názornost si můžeme relace mezi množinami znázorňovat graficky, zejména jsou-li množiny konečné. Je-li například ρ relací mezi A a B, pak si znázorníme prvky obou množin jako body v rovině a bod $r \in A$ spojíme orientovanou šipkou s bodem $s \in B$ právě tehdy, když $(r, s) \in \rho$. Například pro relace ρ, σ z příkladu 4.3. dostáváme "graf":



Obr. 2.

Pomoci těchto "grafů" si můžeme schematicky znázornit i další pojmy, jako například skládání relací. Je zřejmé, že při relaci $\sigma \circ \rho$ vede orientovaná šipka z bodu $r \in A$ do bodu $t \in C$ právě když tuto šipku lze "složit" ze šipky patřící do relace ρ a šipky patřící do relace σ.

Někdy je také užitečné danou relaci ρ mezi konečnými množinami A a B znázornit tabulkou, která má dva řádky a tolik sloupců, kolik uspořádaných dvojic z $A \times B$ patří do ρ. Je-li $(a, b) \in \rho$, pak prvek a napíšeme do horního řádku ta-

bulky a prvek b napíšeme pod něj. Například pro relace ρ a σ z příkladu 4.3. dostáváme tabulky:

ρ :

a	c	c
y	y	z

σ :

x	x	x	x	y	y
k	l	m	n	k	n

Věta 4.1. *Nechť ρ je relace mezi A a B, σ je relace mezi B a C, τ je relace mezi C a D. Pak platí:*

$$\tau \circ (\sigma \circ \rho) = (\tau \circ \sigma) \circ \rho .$$

[D ů k a z: je zřejmé, že $\tau \circ (\sigma \circ \rho)$ i $(\tau \circ \sigma) \circ \rho$ jsou relace mezi A a D; jejich rovnost dokazujeme jakožto množinovou rovnost.

"$\subseteq$" nechť $(x, y) \in \tau \circ (\sigma \circ \rho)$ libovolné; pak podle definice složené relace existuje $c \in C$ tak, že $(x, c) \in \sigma \circ \rho \wedge (c, y) \in \tau$, a tedy existuje $b \in B$ tak, že $(x, b) \in \rho \wedge (b, c) \in \sigma$. Nyní opět užitím definice složené relace dostáváme, že $(b,y) \in \tau \circ \sigma$ a konečně, že $(x, y) \in (\tau \circ \sigma) \circ \rho$. Dohromady tedy: $\tau \circ (\sigma \circ \rho) \subseteq (\tau \circ \sigma) \circ \rho$.

"$\supseteq$" Inkluse $\tau \circ (\sigma \circ \rho) \supseteq (\tau \circ \sigma) \circ \rho$ se dokáže zcela analogicky.]

Definice. Nechť ρ je relace mezi množinami A a B. Relace ρ^{-1} mezi množinami B a A definovaná vztahem

$$\rho^{-1} = \{(u, v) \in B \times A \mid (v, u) \in \rho\}$$

se nazývá **relace inverzní** k relaci ρ.

Poznámka: z předchozí definice plyne, že $(u, v) \in \rho^{-1}$ právě tehdy, když $(v, u) \in \rho$. Znamená to tedy, že

$$\text{Dom } \rho^{-1} = \text{Im } \rho , \qquad \text{Im } \rho^{-1} = \text{Dom } \rho .$$

Znázorníme-li si relaci ρ "grafem", pak zřejmě "graf" relace ρ^{-1} získáme tak, že všechny šipky z ρ ponecháme, ale změníme pouze jejich orientaci.

Věta 4.2.: *Nechť ρ je relace mezi A a B, σ je relace mezi B a C. Pak platí:*

1. $(\rho^{-1})^{-1} = \rho$
2. $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.

[D ů k a z: 1. je zřejmé z definice inverzní relace

2. zřejmě $(\sigma \circ \rho)^{-1}$ i $\rho^{-1} \circ \sigma^{-1}$ jsou relace mezi C a A; jejich rov-

nost dokazujeme jakožto množinovou rovnost.

"$\subseteq$" nechť $(u, v) \in (\sigma \circ \rho)^{-1}$ libovolné; potom podle definice inverzní relace je $(v, u) \in \sigma \circ \rho$ a podle definice složené relace pak existuje $b \in B$ tak, že $(v, b) \in \rho \wedge (b, u) \in \sigma$. Potom však $(b, v) \in \rho^{-1} \wedge (u, b) \in \sigma^{-1}$ a podle definice složené relace je $(u, v) \in \rho^{-1} \circ \sigma^{-1}$. Dohromady tedy $(\sigma \circ \rho)^{-1} \subseteq \rho^{-1} \circ \sigma^{-1}$.

"$\supseteq$" Inkluse $(\sigma \circ \rho)^{-1} \supseteq \rho^{-1} \circ \sigma^{-1}$ se dokáže zcela analogicky.]

Na závěr tohoto paragrafu se budeme zabývat speciálním, avšak v praxi se často vyskytujícím typem relace mezi A a B, a sice případem, kdy $A, B \neq \phi$ a $A = B$.

Definice: Nechť M je neprázdná množina. Pak libovolná podmnožina ρ kartézského součinu $M \times M$ se nazývá **relace na množině** M. Množinu M spolu s relací ρ označíme symbolem (M, ρ) a budeme říkat, že (M, ρ) je množina s relací.

Pro $x, y \in M$ budeme místo $(x, y) \in \rho$ psát obvykle $x \rho y$, resp. místo $(x, y) \notin \rho$ budeme psát $x \bar{\rho} y$.

Příklad 4.4.

1. Nechť $M = \{a, b, c, d\}$; pak $\rho = \{(a, b), (b, a), (b, b), (b, c)\}$ je relace na množině M.

2. Nechť M je libovolná (neprázdná) množina. Pak
   a) prázdná relace $\rho = \phi$ je relací na M
   b) univerzální relace $\rho = M \times M$ je relací na M
   c) množina $\{(m, m) \mid m \in M\}$ je relací na M, kterou nazýváme relace rovnosti (na M) a označujeme symbolem ι (řecké písmeno jota). Je charakterizována tím, že každý prvek z M je v relaci právě sám se sebou.

3. Nechť $M = 2^A$, kde A je libovolná množina. Potom je $M \neq \phi$ a množina
   $$\{(X, Y) \mid X, Y \in 2^A \wedge X \subseteq Y\}$$
je relace na 2^A, kterou nazýváme **relace inkluse** a obvykle ji označujeme sybolem $\subseteq$.

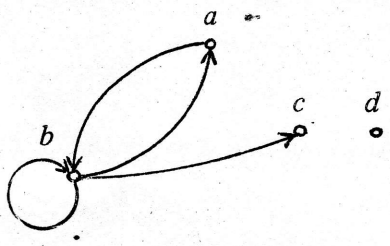
4. Nechť $M = \mathbf{N}$ je množina všech přirozených čísel. Pak množina
   $$\{(a, b) \mid a, b \in \mathbf{N} \wedge a \text{ dělí } b\}$$
je relace na $\mathbf{N}$, kterou nazýváme **relace dělitelnosti** a obvykle ji označujeme symbolem $|$.

5. Nechť $M = \mathbf{Z}$ je množina všech celých čísel, nechť m je pevné přirozené číslo. Pak množina:
   $$\{(a, b) \mid a, b \in \mathbf{Z} \wedge a \equiv b \pmod{m}\}$$

je relace na $\mathbf{Z}$, kterou nazýváme **relace kongruence podle modulu** m.

Poznámka: Schematické znazorňování relací na množině (zejména, je-li množina konečná) můžeme provést graficky, podobným způsobem jako u relací mezi množinami. Je-li (M, ρ) množina s relací, pak prvky množiny M znázorníme jako body v rovině a z bodu x uděláme orientovanou šipku do bodu y právě tehdy, když $x\rho y$. Přitom je samozřejmě možné, že šipka začíná i končí v témže bodě. Takové šipky se nazývají smyčky. Takto vzniklý obrázek obvykle nazýváme **uzlový graf relace** ρ. Například relace ρ z příkladu 4.4.1. má uzlový graf na obr. 3.

Výhodné je rovněž vyjadřování relace ρ na množině M pomocí tabulky, kterou sestrojíme takto: do záhlaví řádků a sloupců vypíšeme prvky množiny M (ve stejném pořadí). Do průsečíku řádku x a sloupce y pak napíšeme 1, je-li $x\rho y$, resp. napíšeme 0, je-li $x\overline{\rho}y$. Například **tabulka relace** ρ z příkladu 4.4.1. je znázorněna tabulkou 4.



Obr. 3

	a	b	c	d
a	0	1	0	0
b	1	1	1	0
c	0	0	0	0
d	0	0	0	0

Tab. 4

Později uvidíme, že některé speciální relace je výhodné znázorňovat i jiným způsobem. Nyní si nejprve popíšeme základní speciální typy relací na množině.

Definice. Nechť (M, ρ) je množina s relací. Řekneme, že relace ρ je

(i) reflexivní, jestliže: $x \in M$ libovolný $\Rightarrow x\rho x$

(ii) symetrická, jestliže: $x, y \in M \wedge x\rho y \Rightarrow y\rho x$

(iii) antisymetrická, jestliže: $x, y \in M \wedge x\rho y \wedge y\rho x \Rightarrow x = y$

(iv) transitivní, jestliže: $x, y, z \in M \wedge x\rho y \wedge y\rho z \Rightarrow x\rho z$

(v) úplná, jestliže: $x, y \in M$ libovolné $\Rightarrow x\rho y \vee y\rho x$.

Poznámka. Předchozí definice bude hrát v dalším zásadní roli, a proto je nutné ji bezpečně zvládnout. Ukažme si, jak se poznají jednotlivé typy relací z uzlového grafu (viz a)), resp. z tabulky relace (viz b)):

reflexivní: a) každý bod je opatřen smyčkou

b) v hlavní diagonále tabulky jsou jedničky

symetrická: a) mezi dvěma různými body jsou buď dvě nebo žádná šipka

b) tabulka je symetrická podle hlavní diagonály

antisymetrická: a) mezi dvěma různými body je buď jedna nebo žádná šipka

b) dvě různá políčka symetrická podle hlavní diagonály neobsahují dvě jedničky

úplná: a) každé dva body jsou spojeny šipkou (tedy mimo jiné je každý bod opatřen smyčkou)

b) v diagonále jedničky a dvě různá políčka, symetrická podle diagonály obsahují alespoň jednu jedničku.

U transitivní relace je situace zejména v tabulce poněkud složitější (i když je možné ji také popsat), a proto se jí zde nebudeme zabývat.

Jinou charakterizaci těchto základních typů relací na množině nám podává následující věta.

Věta 4.3. *Nechť* (M, ρ) *je množina s relací. Pak platí:*

1. *relace* ρ *je reflexivní* $\Leftrightarrow$ $\iota \subseteq \rho$ *(kde* ι *značí relaci rovnosti na* M*)*
2. *relace* ρ *je symetrická* $\Leftrightarrow$ $\rho = \rho^{-1}$
3. *relace* ρ *je antisymetrická* $\Leftrightarrow$ $\rho \cap \rho^{-1} \subseteq \iota$
4. *relace* ρ *je transitivní* $\Leftrightarrow$ $\rho \circ \rho \subseteq \rho$

[D ů k a z: 1. zřejmé

2. "$\Rightarrow$" nechť ρ je symetrická relace na M. Dokážeme, že $\rho = \rho^{-1}$ (jako množinovou rovnost). Nechť tedy $(x, y) \in \rho$ libovolné; tzn. $x\rho y$. Potom je $y\rho x$, neboli $(y, x) \in \rho$, odkud $(x, y) \in \rho^{-1}$. Platí tedy $\rho \subseteq \rho^{-1}$ a opačná inkluse se dokáže analogicky. Dohromady pak je $\rho = \rho^{-1}$.

"$\Leftarrow$" předpokládejme, že $\rho = \rho^{-1}$; nechť $x\rho y$, tzn. $(x, y) \in \rho = \rho^{-1}$. Potom však $(y, x) \in \rho$, tzn. $y\rho x$ a relace ρ je symetrická.

3. "$\Rightarrow$" nechť ρ je antisymetrická relace na M; nechť dále $(x, y) \in \rho \cap \rho^{-1}$ libovolné, tzn. $x\rho y \wedge y\rho x$. Ale ρ je antisymetrická, a tedy $x = y$, neboli $(x, y) \in \iota$. Tedy $\rho \cap \rho^{-1} \subseteq \iota$.

"$\Leftarrow$" nechť $\rho \cap \rho^{-1} \subseteq \iota$; nechť dále $x\rho y \wedge y\rho x$. To ale znamená, že $(x, y) \in \rho \cap \rho^{-1}$, a tedy $(x, y) \in \iota$, neboli $x = y$. Relace ρ je pak antisymetric-

ká.

4. "⇒" nechť ρ je transitivní a nechť $(x, y) \in \rho \circ \rho$ libovolné. Pak podle definice složené relace existuje $w \in M$ tak, že $x\rho w \wedge w\rho y$. Ale z transitivnosti relace ρ plyne, že $x\rho y$, neboli $(x, y) \in \rho$. Je tedy $\rho \circ \rho \subseteq \rho$.

"⇐" nechť $\rho \circ \rho \subseteq \rho$ a nechť $x\rho y \wedge y\rho z$. Podle definice složené relace pak $(x, z) \in \rho \circ \rho \subseteq \rho$, tzn. $x\rho z$. Relace ρ je tedy transitivní.]

Poznamenejme ještě, že symetrie a antisymetrie se navzájem nevylučují (například relace rovnosti na M je zároveň symetrická i antisymetrická) a dále, že úplná relace musí být vždy reflexivní.

Následující tabulka 5 nám udává, které z výše definovaných vlastností mají množiny s relací z příkladu 4.4. (označované zde 1. - 5. stejně jako v příkladu 4.4.). Je užitečné si každou jednotlivou odpověď podrobně samostatně ověřit!

	1.	2.			3.	4.	5.
		a)	b)	c)			
reflexivní	ne	ne	ano	ano	ano	ano	ano
symetrická	ne	ano	ano	ano	**)	ne	ano
antisymetrická	ne	ano	*)	ano	ano	ano	ne
transitivní	ne	ano	ano	ano	ano	ano	ano
úplná	ne	ne	ano	*)	***)	ne	ne

*) ano, je-li M jednoprvková, jinak ne
**) ano, je-li $A = \phi$, jinak ne
***) ano, je-li A prázdná nebo jednoprvková, jinak ne

Tabulka 5

Relace na množině M tak jak byla v tomto paragrafu definována, se také někdy nazývá "binární relace". Tento pojem je možno zobecnit na pojem tzv. "n-ární relace na množině M", která je pak definována jako libovolná podmnožina kartézského součinu $M^n = M \times M \times \ldots \times M$ (n-krát), pro libovolné pevné přirozené číslo n. Ve speciálních případech pak dostáváme:

pro $n = 1$ tzv. unární relaci (což je tedy libovolná podmnožina množiny M)

pro $n = 2$ binární relaci, s níž jsme pracovali výše,

pro $n = 3$ tzv. ternární relaci (což je libovolná podmnožina $M \times M \times M$), atd.

§ 5. Zobrazení.

Pojem zobrazení množiny A do množiny B se zavádí na střední škole obvykle jakožto speciální typ relace mezi množinami A a B.

Definice. Nechť A, B jsou libovolné neprázdné množiny, nechť f je relace mezi množinami A a B, splňující vlastnost:
(1) ke každému $x \in A$ existuje jediné $y \in B$ tak, že $(x, y) \in f$.
Pak uspořádanou trojici (A, B, f) nazýváme **zobrazení množiny A do množiny B.**

Pojem zobrazení je výše uvedeným způsobem definován naprosto jasně a přesně jakožto uspořádaná trojice množin s jistými vlastnostmi. Ukazuje se však, že pojem sám a především pak jeho vlastnosti se v řeči relací vyjadřují poněkud nenázorně a jejich dobré pochopení činí často potíže. Bude proto užitečné přidat k definici zobrazení určité úmluvy tak, aby práce s tímto pojmem byla jednodušší a názornější.

Úmluva: Nechť (A, B, f) je zobrazení množiny A do množiny B. Pak místo (A, B, f) budeme psát $f : A \to B$ a budeme hovořit o zobrazení f množiny A do množiny B nebo jen stručně o zobrazení f.

Množinu A (resp. B) budeme nazývat **definiční obor** (resp. **obor hodnot**) **zobrazení** f.

Místo $(x, y) \in f$ budeme psát $f(x) = y$, při čemž prvek y se bude nazývat **obraz prvku** x (při zobrazení f) a prvek x se bude nazývat vzor prvku y (při zobrazení f).

Po této naší úmluvě můžeme pak definici zobrazení vyslovit ve zjednodušené formě následovně:

Definice. Nechť A, B jsou libovolné neprázdné množiny. Zobrazením f množiny A do množiny B (symbolicky $f : A \to B$) rozumíme předpis f, který každému prvku $x \in A$ přiřazuje právě jeden prvek $y \in B$; píšeme $f(x) = y$.

Poznámka: z toho, co bylo doposud řečeno vidíme, že k zadání zobrazení je nutné zadat:

a) definiční obor A

b) obor hodnot B

c) předpis f, který každému prvku z A přiřazuje jediný prvek z B.

Při tom předpis f je možno zadat různými způsoby, jak ukáží následující příklady.

Příklad 5.1.: definujme zobrazení $f : A \to B$ takto:

1. $A = \{a, b, c, d, e\}$; $B = \{u, v, w\}$; položme: $f(a) = u$, $f(b) = u$, $f(c) = u$, $f(d) = w$, $f(e) = w$

2. $A = \mathbf{Z}$; $B = \mathbf{S}$ (množina všech sudých celých čísel); položme $f(x) = 2x$ pro každé $x \in \mathbf{Z}$

3. $A = \mathbf{N}$; $B = \mathbf{Z}$; položme:

$$f(x) = \begin{cases} x - 1 & \text{pro } 1 \leqslant x \leqslant 9 \\ 10 & \text{pro } x = 10 \\ x + 2 & \text{pro } x \geqslant 11 \end{cases} \qquad x \in \mathbf{N}$$

4. $A = \mathbf{R}$; $B = \mathbf{R}$; položme $f(x) = \sin x$, pro každé $x \in \mathbf{R}$

5. $A = \mathbf{R}$; $B = [-1, 1]$; položme $f(x) = \sin x$, pro každé $x \in \mathbf{R}$

Poznámka: Z definice zobrazení plyne, že dvě zobrazení $f : A \to B$, $g : C \to D$ jsou rovná (stručně píšeme $f = g$), jestliže

a) $A = C$ (tj. rovnají se definiční obory)

b) $B = D$ (tj. rovnají se obory hodnot)

c) $f(x) = g(x)$ pro každé $x \in A$ (tj. rovnají se předpisy).

V opačném případě (tj. není-li splněna alespoň jedna z předchozích tří podmínek) zobrazení nejsou rovná (stručně píšeme $f \neq g$).

Vidíme tedy, že například zobrazení z příkladu 5.1.4. a 5.1.5. nejsou rovná, i když předpis v obou případech zní stejně.

Poznámka:

1. Je-li $A \subseteq \mathbf{R}$, $B \subseteq \mathbf{R}$, pak zobrazení $f : A \to B$ se obvykle nazývá (reálná) **funkce** (jedné reálné proměnné). Tato zobrazení se podrobně studují v matematické analýze.

2. Zobrazení, jehož definičním oborem je množina $\mathbf{N}$ všech přirozených čísel, se obvykle nazývá **posloupnost**. Tedy například zobrazení f z příkladu 5.1.3. je posloupnost. U posloupnosti bývá zvykem značit obrazy prvků pomocí indexů, tzn. místo $f(n)$ psát například f_n apod.

3. **Systém všech zobrazení množiny A do množiny B** budeme v dalším označovat

symbolem B^A. Je tedy

$$B^A = \{f \mid f : A \to B\}.$$

Je-li například $A = \{a, b, c\}$ tříprvková a $B = \{x, y\}$ dvouprvková množina, pak má množina B^A celkem $2^3 = 8$ prvků, tj. existuje právě 8 různých zobrazení A do B (zkuste si je všechny vypsat!) Obecně lze pak ukázat, že má-li množina A n prvků a množina B má s prvků, pak B^A má s^n prvků (což svým způsobem zdůvodňuje použité označení).

4. Pro úplnost ještě poznamenejme, že někdy se (i na střední škole) při studiu zobrazení vychází z obecnějšího pojmu "zobrazení f z množiny A do množiny B" (všimněte si, že je zde navíc písmenko "z"), který se od naší úvodní definice zobrazení liší pouze v tom, že podmínka (1) je nahrazena obecnější podmínkou (2):

(2) ke každému $x \in A$ existuje nejvýše jedno $y \in B$ tak, že $(x, y) \in f$.

My však tento pojem v dalším nebudeme potřebovat, a proto se jím nezabýváme.

Definice: Nechť $f : A \to B$ je zobrazení. Pak zobrazení f se nazývá

(i) **injektivní** (nebo též prosté), jestliže každý prvek z množiny B má (při zobrazení f) nejvýše jeden vzor (tj. jeden nebo žádný)

(ii) **surjektivní** (nebo též zobrazení na), jestliže každý prvek z množiny B má (při zobrazení f) alespoň jeden vzor (tj. jeden nebo více)

(iii) **bijektivní** (nebo též vzájemně jednoznačné), je-li zároveň injektivní i surjektivní, tzn. jestliže každý prvek z B má při zobrazení f právě jeden vzor.

Poznámka: O každém z výše definovaných typů zobrazení je nutné mít jasnou názornou představu. Je tedy m.j. nutné vědět jak se dokazuje, že nějaké konkretní zobrazení je či není injektivní či surjektivní.

Je-li tedy $f : A \to B$ zobrazení a chceme-li dokázat, že

a) f je injektivní,

pak pro libovolné dva prvky $a_1, a_2 \in A$, které jsou různé, tj. $a_1 \neq a_2$, dokážeme, že $f(a_1) \neq f(a_2)$.

Někdy je v tomto případě technicky výhodnější postupovat ekvivalentním způsobem, tj. vezmeme dva prvky $a_1, a_2 \in A$ takové, že $f(a_1) = f(a_2)$ a dokážeme odsud, že $a_1 = a_2$.

b) f není injektivní,

pak musíme najít dva (konkretní) prvky $a_1, a_2 \in A$ takové, že $a_1 \neq a_2$ a $f(a_1) = f(a_2)$

c) f je surjektivní,

pak vezmeme libovolný (obecný) prvek $b \in B$ a najdeme k němu vzor, tj. prvek $a \in A$

takový, že $f(a) = b$

d) f není surjektivní,

pak musíme v B nalézt konkretní prvek, který při zobrazení f nemá žádný vzor.

Příklad 5.2.:

1. Nechť A je libovolná neprázdná množina. Zobrazení $id_A : A \to A$ definované: $id_A(x) = x$, pro každé $x \in A$, se nazývá **identické zobrazení** (nebo též identita) na množině A.

Zřejmě id_A je bijektivní zobrazení.

2. Nechť A, B jsou libovolné neprázdné množiny; nechť $b_0 \in B$ je pevný prvek. Zobrazení $f : A \to B$ definované: $f(x) = b_0$, pro každé $x \in A$, se nazývá **konstantní zobrazení.**

Zřejmě platí, že konstantní zobrazení je injektivní (resp. surjektivní, resp. bijektivní) právě když A (resp. B resp. A i B) je jednoprvková množina.

3. Zobrazení f definovaná v příkladu 5.1. mají tyto vlastnosti:
   1. není injektivní, není surjektivní
   2. je bijektivní
   3. je injektivní, není surjektivní
   4. není injektivní, není surjektivní
   5. není injektivní, je surjektivní.

Definice: Nechť $f : A \to B$ je bijektivní zobrazení. Definujme zobrazení $f^{-1} : B \to A$ takto: pro libovolné $b \in B$ položíme $f^{-1}(b) = a$, kde $a \in A$ je vzor prvku b při zobrazení f (z definice bijektivního zobrazení plyne, že takovýto prvek a existuje, a to jediný). Zobrazeni f^{-1} nazýváme **inverzní zobrazení** k f.

Příklad 5.3.:

1. Identické zobrazení $id_A : A \to A$ je bijektivní (viz příklad 5.2.1). Pro inverzní zobrazení $(id_A)^{-1} : A \to A$ zřejmě platí: $(id_A)^{-1} = id_A$

2. Zobrazení $f : \mathbf{Z} \to \mathbf{S}$ (sudá čísla) definované vztahem $f(x) = 2x$, pro $\forall x \in \mathbf{Z}$ je bijektivní (viz příklady 5.1.2. a 5.2.3.). Inverzní zobrazení $f^{-1} : \mathbf{S} \to \mathbf{Z}$ je pak zřejmě definováno vztahem $f^{-1}(s) = \frac{s}{2}$, pro $\forall s \in \mathbf{S}$ (tj. s sudé).

Věta 5.1.: *Nechť* $f : A \to B$ *je bijektivní zobrazení. Pak platí:*

1. $f^{-1} : B \to A$ *je bijektivní zobrazení*

2. $(f^{-1})^{-1} = f$

[D ů k a z: 1: plyne ihned z definice inverzního a bijektivního zobrazení

2: zřejmě $(f^{-1})^{-1} : A \to B$ a podle předpokladu je $f : A \to B$. U obou zobrazení jsou tedy rovné definiční obory i obory hodnot a zbývá dokázat rovnost předpisů. Nechť $x \in A$ libovolné a nechť $f(x) = y \in B$. Pak ale $f^{-1}(y) = x$, odkud dostáváme: $(f^{-1})^{-1}(x) = y = f(x)$.]

Definice: Nechť $f : A \to B$, $g : B \to C$ jsou zobrazení. Zobrazení $(g \circ f) : A \to C$ definované:

$$(g \circ f)(x) = g(f(x)) \qquad \text{pro každé } x \in A$$

se nazývá **složené zobrazení** ze zobrazení f a g (v tomto pořadí).

Věta 5.2.: *Nechť* $f : A \to B$, $g : B \to C$, $h : C \to D$ *jsou zobrazení. Pak platí:*

$$h \circ (g \circ f) = (h \circ g) \circ f .$$

[D ů k a z: zřejmě je $h \circ (g \circ f) : A \to D$, resp. $(h \circ g) \circ f : A \to D$. Dále, pro libovolné $x \in A$ je $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) =$ $= ((h \circ g) \circ f)(x)$, odkud již dostáváme tvrzení věty.]

Poznámka: Rozebereme-li si definici složeného zobrazení, pak zjistíme, že skládání zobrazení není vlastně nic jiného, než v předchozím paragrafu popisované skládání relací (je nutno si pouze uvědomit, že složením dvou relací, které mají vlastnost (1) obdržíme relaci, která má opět vlastnost (1)). Z tohoto hlediska je potom V.5.2. pouze specielním případem V.4.1. (a nebylo ji tedy nutné ani dokazovat).

Dále vidíme, že o skládání dvou zobrazení hovoříme pouze v případě, že definiční obor druhého zobrazení je roven oboru hodnot prvního zobrazení. Schematicky zachycuje celou situaci obr. 4. Poznamenejme ještě, že symbol $g \circ f$ čteme buď "g kolečko f" nebo "g po f".

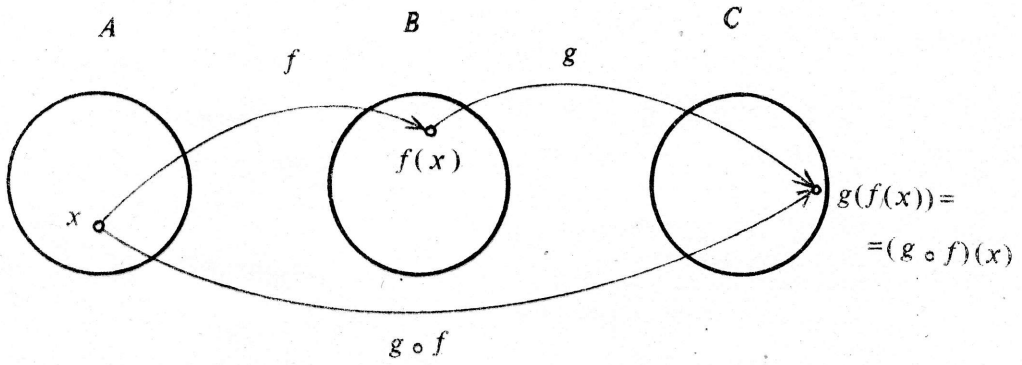
Věta 5.3. *Nechť* $f : A \to B$ *je zobrazení. Pak platí:*

1. $f \circ id_A = f ; \qquad id_B \circ f = f$

2. f *je bijektivní* $\Rightarrow f^{-1} \circ f = id_A , \qquad f \circ f^{-1} = id_B .$

[D ů k a z: 1. zřejmé, dostaneme bezprostředním rozepsáním

2. je-li f bijektivní zobrazení, pak existuje inverzní zobrazení $f^{-1}: B \to A$, a platí: $f^{-1} \circ f : A \to A$. Zřejmě je $id_A : A \to A$. Dále, nechť $x \in A$ je libovolný; potom: $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = id_A(x)$, a platí tedy $f^{-1} \circ f = id_A$. Zbývající rovnost se dokáže analogicky.]



Obr. 4

Věta 5.4.: *Nechť $f : A \to B$, $g : B \to A$ jsou zobrazení taková, že $g \circ f = id_A$. Potom platí: f je injektivní zobrazení a g je surjektivní zobrazení.*

[D ů k a z: nechť $g \circ f = id_A$.

I. dokážeme, že f je injektivní zobrazení. Nechť $a_1, a_2 \in A$ tak, že $f(a_1) = f(a_2)$. Potom: $a_1 = id_A(a_1) = (g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2) = id_A(a_2) = a_2$, a tedy f je skutečně injektivní.

II. dokážeme, že g je surjektivní zobrazení. Nechť $x \in A$ je libovolný prvek. Potom: $x = id_A(x) = (g \circ f)(x) = g(f(x))$, tzn. prvek $f(x)$ je vzorem prvku x při zobrazení g, a tedy g je surjektivní.]

Poznámka: připomeňme, že tvrzení předchozí věty není možné zesílit, tzn., že zobrazení f ani g nemusí být obecně bijektivní, jak by se snad mohlo na první pohled zdát. Ukažme si to na následujícím příkladu.

Nechť $A = B = \mathbf{N}$ (množina všech přirozených čísel); nechť zobrazení $f : A \to B$,

resp. $g : B \to A$ jsou definována:

$$f(x) = x + 1, \quad \text{pro } \forall x \in A, \text{ resp. } \quad g(x) = \begin{cases} 1 & \text{pro } x = 1 \\ x - 1 & \text{pro } x \geqslant 2 \end{cases}$$

(zkuste si nejprve samostatně obě zobrazení graficky znázornit!). Zřejmě je $g \circ f = id_A$ (uvažme, že $(g \circ f)(x) = g(f(x)) = g(x + 1) = (x + 1) - 1 = x$), přičemž však f není surjektivní (neboť $1 \in B$ nemá při zobrazení f žádný vzor) a g není injektivní (neboť $1 \neq 2$ a $g(1) = g(2)$), a tedy f ani g nejsou bijektivní.

Důsledek: *Nechť $f : A \to B$, $g : B \to A$ jsou zobrazení. Pak platí:* $g \circ f = id_A$, $f \circ g = id_B \Leftrightarrow$ *f, g jsou bijektivní a* $g = f^{-1}$.

[D ů k a z: "⇒" použijeme-li dvakrát předchozí větu, dostáváme, že f i g jsou bijektivní. Dále zřejmě $g : B \to A$, $f^{-1} : B \to A$. Dokážeme rovnost předpisů. Nechť $b \in B$ libovolné; potom (protože f je bijektivní) existuje jediný prvek $a \in A$ s vlastností: $f(a) = b$. Pak ale $f^{-1}(b) = a = id_A(a) = (g \circ f)(a) = g(f(a)) = g(b)$. Tedy $g = f^{-1}$.

"⇐" plyne z V.5.3.2.]

Definice: Nechť $f : A \to B$ je zobrazení; nechť M je neprázdná podmnožina definičního oboru A (tzn. $\phi \neq M \subseteq A$). Pak zobrazení $h : M \to B$ definované: $h(m) = f(m)$, pro každé $m \in M$, se nazývá **zúžení zobrazení** f na množinu M a obvykle se značí symbolem $f|M$.

Poznámka: Je-li dáno zobrazení $f : A \to B$, pak vidíme, že při konstrukci zúženého zobrazení $f|M : M \to B$ se změní pouze definiční obor. Je však nutné si uvědomit, že zúžením zobrazení se mohou podstatně změnit některé jeho základní vlastnosti, jak ukazuje následující příklad.

Příklad 5.4.: Nechť $f : \mathbf{R} \to \mathbf{R}$ je zobrazení definované: $f(x) = x^2$, pro $\forall x \in \mathbf{R}$. Nechť M je množina všech kladných reálných čísel. Pak zúžení $f|M : M \to \mathbf{R}$ je definované $(f|M)(x) = x^2$, pro $\forall x \in M$. Při tom zobrazení f není injektivní, zatímco zúžení $f|M$ injektivní je.

§ 6. Uspořádané množiny.

V tomto a v následujícím paragrafu budeme blíže studovat relace na (neprázdné) množi- M, které splňují některé z dříve definovaných speciálních vlastností.

Definice: Nechť (M, ρ) je množina s relací, která je reflexivní, antisymetrická a transitivní. Pak se relace ρ nazývá **uspořádání** a (M, ρ) se nazývá **uspořádaná množina.**

Je-li navíc relace ρ úplná, nazývá se pak **lineární uspořádání** a (M, ρ) se nazývá **lineárně uspořádaná množina** nebo krátce řetězec.

Úmluva: 1: relaci uspořádání budeme v dalším při obecných úvahách obvykle značit symbolem $\leqslant$ (čti "menší nebo rovno"). Poznamenejme, že takto použitý symbol $\leqslant$ nemá zde obecně nic společného se srovnáváním čísel podle velikosti, které se na střední škole znázorňuje též symbolem $\leqslant$.

2: Místo $x \leqslant y$ budeme podle potřeby též psát $y \geqslant x$ (obojí znamená, že prvek x je v relaci uspořádání s prvkem y).

3: Pro: $x \leqslant y \wedge x \neq y$ budeme používat stručného označení $x < y$ nebo též $y > x$ (čti "x je menší než y").

Takto zavedená označení zjednoduší naše další vyjadřování (uvědomme si výhodnost použitého symbolu; se symbolem ρ by zřejmě podobné "triky" nebyly možné). Následující příklady si samostatně podrobně zdůvodněte!

Příklad 6.1.

1. Relace inkluse $\subseteq$ na množině 2^A (viz příklad 4.4.3) je relací uspořádání. Při tom $(2^A, \subseteq)$ je lineárně uspořádaná množina právě když množina A je prázdná nebo jednoprvková (tj. právě když 2^A je jednoprvková nebo dvouprvková).

2. Relace dělitelnosti $|$ na množině $\mathbf{N}$ (viz příklad 4.4.4.) je relací uspořádání. Při tom $(\mathbf{N}, |)$ není lineárně uspořádaná množina.

3. Na množině $\mathbf{N}$ všech přirozených čísel definujme relaci $\leqslant$ jakožto relaci tzv. "přirozeného uspořádání" (tj. uspořádání čísel podle velikosti, kdy $x \leqslant y$ právě když $y - x$ je nezáporné číslo). Potom relace $\leqslant$ je relací lineárního uspořádání a $(\mathbf{N}, \leqslant)$ je lineárně uspořádaná množina.

Podobně můžeme definovat přirozené uspořádání $\leqslant$ například na množině všech celých

čísel $\mathbf{Z}$, resp. racionálních čísel $\mathbf{Q}$, resp. reálných čísel $\mathbf{R}$ a dostáváme pak lineárně uspořádané množiny $(\mathbf{Z}, \leqslant)$, resp. $(\mathbf{Q}, \leqslant)$, resp. $(\mathbf{R}, \leqslant)$.

Poznámka: Uspořádanou množinu $(M, \leqslant)$ můžeme (zejména, je-li M konečná) graficky znázorňovat následujícím způsobem: prvky množiny M znázorníme jako body v rovině tak, aby v případě, že je $x < y$, ležel bod x níže než bod y. Dva body $x, y \in M$ spojíme úsečkou právě tehdy, když $x < y$ a neexistuje $w \in M$ tak, že $x < w < y$.

Výsledný graf se pak nazývá **hasseovský diagram** uspořádané množiny $(M, \leqslant)$. Vidíme, že jde vlastně o zjednodušený uzlový graf relace $\leqslant$ (jsou vynechány smyčky, které by měly být u každého bodu; dále je vynechána orientace šipek, která je nahrazena umístěním bodu "výše" či "níže" a konečně jsou vynechány "zbytečné" šipky, jejichž existence plyne z transitivity relace $\leqslant$). Pro úplnost poznamenejme, že uvedená konstrukce nedefinuje jednoznačně tvar hasseovského diagramu. Jednu a tutéž uspořádanou množinu je často možné znázornit hasseovskými diagramy různých tvarů tak, že na první pohled nemusí být vůbec zřejmé, že jde o diagramy téže uspořádané množiny. Na druhé straně, známe-li hasseovský diagram uspořádané množiny $(M, \leqslant)$, pak z něj lze relaci $\leqslant$ jednoznačně zpětně zrekonstruovat. Můžeme tedy uspořádanou množinu zadávat hasseovským diagramem.

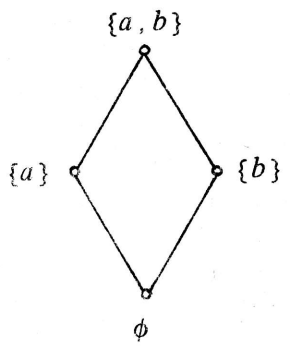
Příklad 6.2.:

1. Nechť $A = \{a, b\}$; pak $2^A = \{\phi, \{a\}, \{b\}, \{a, b\}\}$ a hasseovský diagram uspořádané množiny $(2^A, \subseteq)$ z příkladu 6.1.1. je na obr. 5a.

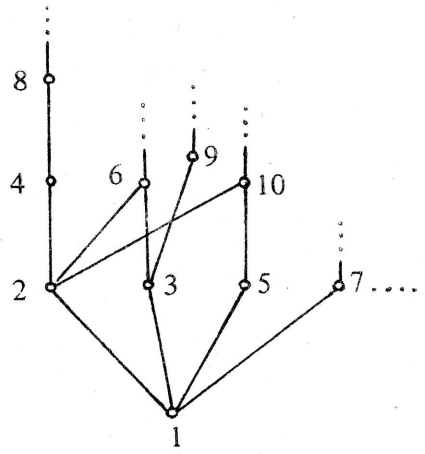
2. Část hasseovského diagramu uspořádané množiny $(\mathbf{N}, |)$ z příkladu 6.1.2. je znázorněna na obr. 5b. Zde si uvědomme, že obrázek nezachycuje ani schematicky celou situaci, neboť z každého čísla x ve skutečnosti vychází nekonečně mnoho úseček (vedoucích do čísel $x.p$, kde p je libovolné prvočíslo, přičemž prvočísel je podle V.3.7. nekonečně mnoho).

3. Hasseovský diagram uspořádané množiny $(\mathbf{N}, \leqslant)$ z příkladu 6.1.3. (tzn. $\leqslant$ zde značí přirozené uspořádání podle velikosti) je na obr. 5c. Přesněji řečeno, na obr. 5c je opět pouze část celého diagramu.

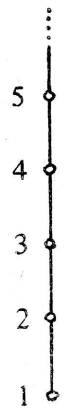
Je jasné, že u nekonečných uspořádaných množin nelze hasseovský diagram nikdy nakreslit celý. Vzniklý obrázek je pak jen více či méně názornou orientační pomůckou (viz obr. 5c, resp. 5b) a někdy dokonce nemá smysl se o něj ani pokoušet (např. u uspořádané množiny $(2^R, \subseteq)$).



Obr. 5a



Obr. 5b



Obr. 5c

Definice: V uspořádané množině $(M, \leqslant)$ se prvek $m \in M$ nazývá:

(i) **nejmenší,** jestliže pro $\forall x \in M$ platí: $m \leqslant x$

(ii) **největší,** jestliže pro $\forall x \in M$ platí: $x \leqslant m$

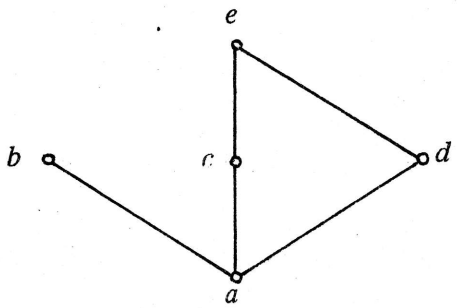
(iii) **minimální,** jestliže neexistuje prvek $x \in M$ s vlastností: $x < m$

(iv) **maximální,** jestliže neexistuje prvek $x \in M$ s vlastností: $m < x$.

Dále, dva prvky $x, y \in M$ se nazývají **srovnatelné,** jestliže $x \leqslant y$ nebo $y \leqslant x$. V opačném případě se prvky x, y nazývají **nesrovnatelné.**

Příklad 6.3.:

1. Nechť uspořádaná množina $(M, \leqslant)$ je zadána hasseovským diagramem na obr. 6.



Obr. 6

Potom: nejmenším prvkem je a; největší prvek neexistuje; minimálním prvkem je a; maximálními prvky jsou b, e. Nesrovnatelné jsou dvojice prvků b, c, resp. b, d, resp. b, e, resp. c, d. Všechny ostatní dvojice prvků jsou srovnatelné prvky.

2. U uspořádaných množin z příkladu 6.2. platí:

1. nejmenší a zároveň jediný minimální prvek je ϕ; největší a zároveň jediný maximální prvek je $\{a, b\}$

2. nejmenší a zároveň jediný minimální prvek je 1; největší ani maximální prvek žádný neexistuje (zdůvodněte proč!)

3. nejmenší a zároveň jediný minimální prvek je 1; největší ani maximální prvek neexistuje.

Poznámka: ověřujeme-li o nějakém prvku $m \in M$, že je minimálním prvkem uspořádané množiny $(M, \leqslant)$, pak obvykle je technicky nejvýhodnější postupovat tak, že dokazujeme implikaci:

$$x \in M \wedge x \leqslant m \Rightarrow x = m .$$

Analogicky, dokazujeme-li, že $m \in M$ je maximální prvek uspořádané množiny $(M, \leqslant)$, pak dokazujeme implikaci:

$$x \in M \wedge m \leqslant x \Rightarrow x = m .$$

Věta 6.1.: *Nechť $(M, \leqslant)$ je uspořádaná množina. Pak platí:*

1. v $(M, \leqslant)$ existuje nejvýše jeden nejmenší prvek a nejvýše jeden největší prvek

2. je-li $m \in M$ nejmenší (resp. největší) prvek, pak m je také minimální (resp. maximální) prvek a žádné další minimální (resp. maximální) prvky v uspořádané množině $(M, \leqslant)$ neexistují

3. $(M, \leqslant)$ je lineárně uspořádaná $\Leftrightarrow$ každé dva prvky množiny M jsou srovnatelné.

[D ů k a z: 1. nechť m, m' jsou nejmenší prvky v $(M, \leqslant)$. Potom je $m \leqslant m'$ (neboť m je nejmenší) a zároveň $m' \leqslant m$ (neboť m' je nejmenší). Z antisymetrie relace $\leqslant$ pak dostáváme, že $m = m'$. Analogicky se ukáže existence nejvýše jednoho největšího prvku.

2. nechť $m \in M$ je nejmenší prvek v $(M, \leqslant)$. Nechť $x \in M \wedge x \leqslant m$. Poněvadž m je nejmenším prvkem, musí však být $m \leqslant x$. Dohromady dostáváme $x = m$, což znamená, že m je minimální prvek v $(M, \leqslant)$. Zbývá ukázat, že žádné další minimální prvky, různé od m, v $(M, \leqslant)$ neexistují. Nechť tedy $m' \in M$ je minimální prvek. Pak je $m \leqslant m'$ (protože m je nejmenší), odkud plyne (z toho, že m' je minimální), že $m = m'$.

3. plyne ihned z definice lineárního uspořádání a definice srovnatelných prvků.]

Poznámka: všimněte si dobře typického obratu použitého v důkazu 1. části předchozí věty. Dokazujeme-li v matematice, že něčeho existuje nejvýše jeden exemplář, pak obvykle postupujeme tak, že předpokládáme existenci dvou exemplářů, o nichž dokážeme, že jsou si rovny.

Věta 6.2.: *Nechť* $(M, \leqslant)$ *je lineárně uspořádaná množina. Potom: prvek* $m \in M$ *je minimální (resp. maximální)* $\Leftrightarrow$ m *je nejmenší (resp. největší).*

[D ů k a z: tvrzení dokážeme pro minimální a nejmenší prvek; pro maximální a největší prvek je důkaz analogický.

"$\Rightarrow$" nechť m je minimální a nechť $x \in M$ je libovolný prvek. Poněvadž $(M, \leqslant)$ je lineárně uspořádaná, je $x \leqslant m$ nebo $m \leqslant x$. Ale z $x \leqslant m$ plyne $x = m$ (neboť m je minimální), a tedy vždycky je $m \leqslant x$, což znamená, že m je nejmenším prvkem.

"$\Leftarrow$" plyne z V.6.1.2.]

Vidíme tedy, že v lineárně uspořádané množině pojmy minimální prvek a nejmenší prvek (resp. maximální prvek a největší prvek) splývají.

§ 7. Ekvivalence a rozklady.

Definice: Nechť (M, ρ) je množina s relací, která je reflexivní, symetrická a transitivní. Pak relace ρ se nazývá **ekvivalence** (na množině M).

Relaci ekvivalence budeme obvykle značit symbolem $\sim$.

Příklad 7.1.:

1. Nechť M je libovolná neprázdná množina. Pak relace rovnosti na M a univerzální relace (viz příklad 4.4.2.c), resp. b)) jsou relacemi ekvivalence na M (jak vyplývá z tabulky 5.).

2. Relace kongruence podle modulu m (viz příklad 4.4.5.) je relací ekvivalence na množině $\mathbf{Z}$ všech celých čísel (opět plyne z tabulky 5.).

3. Nechť $f : A \to B$ je zobrazení; na množině A definujme relaci $\sim$ takto:

pro $x, y \in A$ položme $x \sim y$ právě když $f(x) = f(y)$.

Potom relace $\sim$ je relací ekvivalence na množině A (podrobně si sami dokažte!).

Poznámka: Na dané neprázdné množině M lze zřejmě definovat mnoho různých relací ekvivalence. Označme si symbolem $\&(M)$ množinu všech relací ekvivalence na M. Uvědomíme-li si, že ekvivalence na M je vlastně jistá podmnožina kartézského součinu $M \times M$, pak je jasné, že $(\&(M), \subseteq)$ je uspořádaná množina. Uvážíme-li, že relace rovnosti a univerzální relace jsou ekvivalencemi na M (viz příklad 7.1.1.), pak je již jednoduché ukázat, že relace rovnosti je nejmenším prvkem a univerzální relace je největším prvkem uspořádané množiny $(\&(M), \subseteq)$.

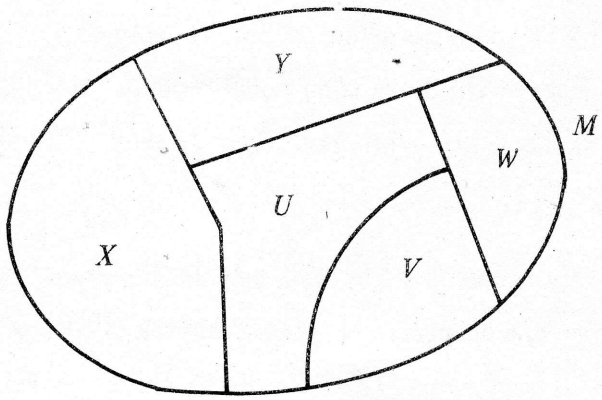
Definice: Nechť M je libovolná neprázdná množina. Pak **rozklad na množině** M je systém $\mathcal{M}$ neprázdných podmnožin množiny M, splňujících:

(i) $X, Y \in \mathcal{M} \wedge X \neq Y \Rightarrow X \cap Y = \phi$

(ii) $\cup X\,(X \in \mathcal{M}) = M$

Prvky systému $\mathcal{M}$ se nazývají třídy rozkladu $\mathcal{M}$.

Poznámka: Nejnázorněji si pojem rozkladu na množině můžeme přiblížit náčrtkem asi takového tvaru, jako je na obr. 7. Na něm je schematicky znázorněn



Obr. 7

rozklad $\mathcal{M} = \{X, Y, U, V, W\}$ mající celkem 5 tříd. Tento obrázek je samozřejmě pouze orientační, protože například jak počet tříd rozkladu, tak počet prvků v jednotlivých třídách může být libovolný (ať už konečný nebo nekonečný). V každém případě je však $\mathcal{M} \neq \phi$.

Dokazujeme-li, že $\mathcal{M}$ je rozklad na množině M, pak z předchozí definice plyne, že je nutné ověřit tři podmínky, a sice, že:

a) každá třída rozkladu je neprázdnou podmnožinou v M

b) dvě různé třídy rozkladu $\mathcal{M}$ jsou disjunktní (tuto podmínku je technicky nejvýhodnější dokazovat tak, že předpokládáme $X, Y \in \mathcal{M}$, $X \cap Y \neq \phi$ a dokážeme pak $X = Y$, obvykle jakožto množinovou rovnost)

c) sjednocení všech tříd rozkladu $\mathcal{M}$ je rovno celé množině M (zde opět technicky dokazujeme pouze inklusi $M \subseteq \cup X$ $(X \in \mathcal{M})$, protože opačná inkluse je triviálně splněna).

Příklad 7.2.:

1. Nechť $M = \mathbf{Z}$; pak množiny $\{x \in \mathbf{Z} \mid x < -2\}$, $\{-2, -1, 0\}$, $\{x \in \mathbf{Z} \mid x$ je sudé kladné$\}$, $\{x \in \mathbf{Z} \mid x$ je liché kladné$\}$ tvoří rozklad na $\mathbf{Z}$. Tento rozklad má 4 třídy, z nichž tři třídy mají nekonečně mnoho prvků a jedna třída má konečně mnoho prvků.

2. Nechť $M = \mathbf{Z}$; pak $\mathcal{M} = \{\{x\} \mid x \in \mathbf{Z}\}$ je rozklad na $\mathbf{Z}$, který má nekonečně mnoho tříd, při čemž každá třída obsahuje právě jeden prvek.

3. Nechť $M = \mathbf{R}$; pro libovolné celé číslo k označme symbolem I_k interval $\langle k, k+1)$, tzn. $I_k = \{x \in \mathbf{R} \mid k \leqslant x < k+1\}$. Potom $\mathcal{M} = \{I_k \mid k \in \mathbf{Z}\}$ je rozklad na $\mathbf{R}$, který má nekonečně mnoho tříd a každá třída má nekonečně mnoho prvků.

Definice: Nechť m je pevné přirozené číslo; označme

(1) $C_i = \{x \in \mathbf{Z} \mid x$ dává po dělení číslem m zbytek $i\}$, $i = 0, 1, \ldots, m-1$.

Pak množina C_i se nazývá **zbytková třída** podle modulu m. Systém všech zbytkových tříd podle modulu m označíme symbolem $\mathbf{Z}_m$. Je tedy

$$\mathbf{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}.$$

Poznámka: Z věty o dělení se zbytkem celých čísel plyne, že zbytkových tříd podle modulu m musí být opravdu právě m (neboť zbytek po dělení číslem m nabývá právě jedné z hodnot $0, 1, \ldots, m-1$). Dále, každá zbytková třída podle modulu m obsahuje zřejmě nekonečně mnoho celých čísel, lišících se navzájem o nějaký celý násobek modulu m. Pokusíme-li se alespoň schematicky si znázornit jednotlivé zbytkové třídy podle modulu m, tj. množiny $C_0, C_1, C_2, \ldots, C_{m-1}$ $(m \geqslant 4)$, dostaneme následující "tabulku":

$$C_0 = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$$

$$C_1 = \{\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots\}$$

$$C_2 = \{\ldots, -2m+2, -m+2, 2, m+2, 2m+2, \ldots\}$$

$$\vdots$$

$$C_{m-1} = \{\ldots, -m-1, -1, m-1, 2m-1, 3m-1, \ldots\}$$

Dále poznamenejme, že někdy bude technicky výhodnější používat definici zbytkové třídy ve tvaru:

(2) $\quad C_i = \{x \in \mathbf{Z} \mid x \equiv i \pmod m\} \qquad i = 0, 1, \ldots, m-1$

(ekvivalentnost vyjádření (1) a (2) plyne z V.3.3. uvědomíme-li si zřejmý fakt, že číslo i (kde $0 \leqslant i \leqslant m-1$) dává po dělení číslem m zbytek i).

Konečně, je nutné velmi důrazně upozornit na to, že není možné navzájem porovnávat množiny zbytkových tříd podle dvou různých modulů. Není tedy například možné říci, že $\mathbf{Z}_3 \subseteq \mathbf{Z}_4$, i když použité označení $\mathbf{Z}_3 = \{C_0, C_1, C_2\}$, $\mathbf{Z}_4 = \{C_0, C_1, C_2, C_3\}$ by k tomu na první pohled mohlo svádět. Zřejmě však například třída $C_0 \in \mathbf{Z}_3$ (tj. $C_0 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$) a třída $C_0 \in \mathbf{Z}_4$ (tj. $C_0 = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$) jsou dvě naprosto rozdílné množiny, atd. Přesně řečeno - každá zbytková třída se váže vždy k jedinému modulu m, což by se správně mělo projevit i v použitém označení (například místo C_i bychom psali třeba C_i^m). Z důvodů stručnosti zápisu však zůstaneme u výše zavedeného označení.

Věta 7.1. : *Nechť m je pevné přirozené číslo. Pak systém zbytkových tříd podle modulu m (tj. $\mathbf{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$) je rozklad na $\mathbf{Z}$.*

[D ů k a z: z definice plyne, že $\mathbf{Z}_m$ je systém neprázdných podmnožin (C_i obsahuje mimo jiné vždy číslo i) množiny $\mathbf{Z}$ a zřejmě platí, že $\bigcup_{i=0}^{m-1} C_i = \mathbf{Z}$. Konečně, nechť $C_i, C_j \in \mathbf{Z}_m$ a $C_i \cap C_j \neq \phi$. Potom existuje $x \in C_i \cap C_j$, tzn. číslo x dává po dělení číslem m zbytek i a současně zbytek j. Ale z věty o dělení se zbytkem víme, že zbytek je určen jednoznačně, tzn. musí být $i = j$, odkud dostáváme, že $C_i = C_j$.]

Mezi ekvivalencemi na množině M a rozklady na M je úzká souvislost, jak se ukáže z následujících vět.

Věta 7.2.: *Nechť* $\sim$ *je relace ekvivalence na množině* M. *Pro* $a \in M$ *položme* $X_a = \{x \in M \mid x \sim a\}$. *Potom systém množin:*

(3) $\{X \mid$ *existuje* $a \in M$ *tak, že* $X = X_a\}$

je rozklad na množině M, *který budeme označovat symbolem* $M/\sim$ *a nazývat* ***rozklad příslušný ekvivalenci*** $\sim$.

[D ů k a z: je zřejmé, že $M/\sim$ je systém neprázdných podmnožin množiny M a že platí $\cup X_a\ (a \in M) = M$ (plyne z toho, že $a \in X_a$). Zbývá tedy dokázat vlastnost (i) z definice rozkladu. Nechť tedy $X_a, X_b \in M/\sim$ a nechť $X_a \cap X_b \neq \phi$, tzn. existuje prvek $w \in X_a \cap X_b$. Dokážeme, že pak $X_a = X_b$.

"$\subseteq$" nechť $x \in X_a$ libovolné; pak je $x \sim a$. Z toho, že $w \in X_a \cap X_b$ plyne, že $w \sim a$, $w \sim b$. Je tedy: $x \sim a \ \wedge\ a \sim w \ \wedge\ w \sim b$, odkud $x \sim b$, neboli $x \in X_b$. Tím jsme dokázali, že $X_a \subseteq X_b$.

"$\supseteq$" dokáže se analogicky.]

Poznámka: zápis (3) je nutno chápat v obvyklém množinovém smyslu, tj. tak, že ve (3) jsou vypsány pouze různé třídy (jinak řečeno, jestliže pro $a, a' \in M$ je $X_a = X_{a'}$, pak ve (3) je ze tříd X_a, $X_{a'}$ zapsána pouze jedna). O skutečném počtu (různých) tříd rozkladu $M/\sim$ se tedy ze zápisu (3) obecně nedá nic říci.

Příklad 7.3.:

1. Nechť M je libovolná neprázdná množina a nechť relace ekvivalence na M je

a) relace rovnosti. Pak rozklad příslušný této ekvivalenci je zřejmě tvaru $\{\{m\} \mid m \in M\}$, tzn. je to rozklad množiny M na jednoprvkové třídy

b) univerzální relace. Pak rozklad příslušný této ekvivalenci je tvaru $\{M\}$, tzn. je to rozklad množiny M mající jedinou třídu, a sice celou množinu M.

2. Nechť $M = \mathbf{Z}$ a za relaci ekvivalence vezmeme relaci $\equiv$ kongruence podle modulu m (viz příklad 4.4.5.). Pak rozklad příslušný této ekvivalenci je roven rozkladu množiny $\mathbf{Z}$ na zbytkové třídy podle modulu m (plyne z (2)), tj. $\mathbf{Z}/\equiv = \{C_0, C_1, \ldots, C_{m-1}\} = \mathbf{Z}_m$.

3. Nechť $f : A \to B$ je zobrazení a nechť $\sim$ je relace ekvivalence na A definovaná v příkladu 7.1.3. (tzn. $x \sim y \Leftrightarrow f(x) = f(y)$). Rozklad $A/\sim$ příslušný této ekvivalenci budeme v dalším nazývat **rozklad příslušný zobrazení** f. Je to tedy rozklad na množině A, jehož třídy jsou tvořeny vždy právě těmi prvky z A, které se zobrazí (pomocí f) na stejný

prvek z B, tzn.

$$A/\sim = \{X \mid \exists a \in A \text{ tak, že } X = X_a\}, \text{ kde } X_a = \{x \in A \mid f(x) = f(a)\}.$$

Věta 7.3.: *Nechť $\mathcal{M}$ je rozklad na množině M. Pro $a, b \in M$ položme:*

$a \sim_{\mathcal{M}} b$ *právě když existuje třída $X \in \mathcal{M}$ tak, že $a, b \in X$.*

Pak relace $\sim_{\mathcal{M}}$ je relací ekvivalence na M, kterou budeme nazývat ***ekvivalence příslušná rozkladu*** $\mathcal{M}$.

[D ů k a z: relace $\sim_{\mathcal{M}}$ je zřejmě reflexivní a symetrická. Dokažme, že je transitivní: nechť $a, b, c \in M$, $a \sim_{\mathcal{M}} b$, $b \sim_{\mathcal{M}} c$. Pak existují třídy $X, Y \in \mathcal{M}$ tak, že $a, b \in X$, $b, c \in Y$. Tedy $b \in X \cap Y$, což znamená, že $X = Y$. Potom však $a, c \in X$, a tedy $a \sim_{\mathcal{M}} c$, tzn. relace $\sim_{\mathcal{M}}$ je transitivní.]

Příklad 7.4.:

1. Nechť M je libovolná neprázdná množina a nechť $\mathcal{M}$ je rozklad na M tvaru:

   a) $\mathcal{M} = \{\{m\} \mid m \in M\}$, tzn. rozklad množiny M na jednoprvkové třídy. Potom ekvivalence příslušná tomuto rozkladu je zřejmě relace rovnosti.

   b) $\mathcal{M} = \{M\}$, tzn. rozklad množiny M mající jedinou třídu (rovnou celé množině M). Pak ekvivalence příslušná tomuto rozkladu je zřejmě univerzální relace.

2. Nechť $M = \mathbf{Z}$ a nechť $\mathcal{M}$ je rozklad na $\mathbf{Z}$ tvaru $\mathcal{M} = \mathbf{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$, tj. rozklad na zbytkové třídy podle modulu m. Pak ekvivalence příslušná tomuto rozkladu je rovna relaci kongruence podle modulu m (neboť podle V.7.3., podle (1) a podle V.3.3. je: $a \sim_{\mathcal{M}} b \Leftrightarrow a, b \in C_i$ pro nějaké $i = 0, 1, \ldots, m-1 \Leftrightarrow a \equiv b \pmod m$).

Poznámka: Uvědomme si, že rozklad příslušný ekvivalenci je pouze jedním pevným rozkladem z mnoha rozkladů, které na množině M můžeme zkonstruovat. Tak například rozklad na množině $\mathbf{Z}$, příslušný relaci kongruence podle modulu m je právě rozklad $\mathbf{Z}_m$ a žádný jiný. Podobně, ekvivalence příslušná rozkladu je opět jediná z mnoha relací ekvivalence, které můžeme na množině M definovat.

Na druhé straně je mezi ekvivalencemi na M a rozklady na M velice úzká spojitost. Přesněji řečeno, vyjdeme-li od jisté ekvivalence na M, utvoříme-li rozklad na M, příslušný této ekvivalenci a potom utvoříme ekvivalenci na M, příslušnou tomuto rozkladu, skončíme u původní ekvivalence, od níž jsme vyšli. Podobně, začneme-li s rozkladem,

dojdeme přes ekvivalenci k němu příslušnou opět k původnímu rozkladu. Přesně popisuje tuto situaci následující věta.

Věta 7.4.: *Nechť M je libovolná neprázdná množina. Pak platí:*

1. je-li $\sim$ ekvivalence na M, pak: $\sim_{M/\sim} = \sim$

2. je-li $\mathcal{M}$ rozklad na M, pak: $M/\sim_{\mathcal{M}} = \mathcal{M}$

[D ů k a z: 1: zřejmě je $\sim \subseteq M \times M$ a $\sim_{M/\sim} \subseteq M \times M$, tzn. dokazovanou rovnost budeme dokazovat jako obyčejnou množinovou rovnost.

"$\subseteq$": nechť $(a, b) \in \sim_{M/\sim}$, tzn. $a \sim_{M/\sim} b$. Pak existuje třída rozkladu $M/\sim$, která obsahuje prvky a, b; například nechť $a, b \in X_u$ (viz (3)). Potom podle definice třídy X_u je $a \sim u$, $b \sim u$, odkud plyne, že $a \sim b$, tzn. $(a, b) \in \sim$ a je tedy $\sim_{M/\sim} \subseteq \sim$.

"$\supseteq$": nechť $(a, b) \in \sim$, tzn. $a \sim b$. Pak je zřejmě $a \in X_a$, $b \in X_a$, kde X_a je jedna ze tříd rozkladu $M/\sim$. Pak ale je $a \sim_{M/\sim} b$, tzn. $(a, b) \in \sim_{M/\sim}$ a tedy $\sim \subseteq \sim_{M/\sim}$.

2: tvrzení dokazujeme opět jako množinovou rovnost.

"$\subseteq$": nechť $X \in M/\sim_{\mathcal{M}}$ je libovolná třída. Pak existuje $a \in M$ tak, že $X = X_a =$ $= \{x \in M \mid x \sim_{\mathcal{M}} a\}$. Ale poslední množina je právě jedna ze tříd rozkladu $\mathcal{M}$, tzn. $X \in \mathcal{M}$. Je tedy $M/\sim_{\mathcal{M}} \subseteq \mathcal{M}$.

"$\supseteq$" nechť $X \in \mathcal{M}$ je libovolná třída. Vezměme libovolný prvek $a \in X$. Pak ale: $X = \{x \in M \mid x \sim_{\mathcal{M}} a\} = X_a \in M/\sim_{\mathcal{M}}$. Je tedy $\mathcal{M} \subseteq M/\sim_{\mathcal{M}}$.]

II. ZÁKLADNÍ ALGEBRAICKÉ STRUKTURY

§ 1. Struktury s jednou operací.

V tomto paragrafu budeme studovat jisté speciální typy zobrazení (tj. vlastně relací), které se nazývají operace. Pojem operace vznikl zobecněním pojmů běžně známých ze střední školy, jako je pojem sčítání či násobení čísel (například reálných) nebo odečítání čísel (například celých), atd. Vidíme, že v těchto případech je vždy libovolné uspořádané dvojici čísel z jisté číselné množiny přiřazeno jediné, přesně určené číslo z téže množiny. Tato úvaha nás vede k následující definici.

Definice: Nechť G je neprázdná množina. Pak libovolné zobrazení $G \times G \to G$ se nazývá **operace na množině** G. Je-li při tomto zobrazení uspořádané dvojici $(a, b) \in G \times G$ přiřazen prvek $c \in G$, pak budeme obvykle psát:

$$a \cdot b = c$$

a hovořit o operaci $\cdot$.

Množina G spolu s operací $\cdot$ se nazývá **grupoid** a označuje symbolem $(G, \cdot)$.

Poznámka:

1. Pro označování operace na G (což je vlastně jisté zobrazení) se ukazuje jako nepraktické používat písmena a symboliku zavedenou v paragrafu o zobrazeních. Vhodnější je používat speciálních symbolů - nejčastěji jsou to:

   α) symbol $\cdot$ (tzv. multiplikativní symbolika); v tomto případě budeme hovořit o operaci "tečka" nebo také o operaci "násobení". Je-li $a \cdot b = c$, pak prvek c budeme nazývat součinem prvků a, b (v tomto pořadí).

   β) symbol $+$ (tzv. aditivní symbolika); v tomto případě budeme hovořit o operaci "křížek" nebo také o operaci "sečítání". Je-li $a + b = c$, pak prvek c budeme nazývat součtem prvků a, b (v tomto pořadí).

Při tom je jistě jasné, že použitý symbol $\cdot$ (resp $+$) obecně nemá nic společného s násobením (resp. sečítáním) čísel.

Poznamenejme ještě, že podle potřeby můžeme operaci na G označovat i jinými, více či méně exotickými symboly, jako například $\circ$, $*$, $\square$, $\triangle$, atd.

2. Z předchozí definice plyne, že grupoid $(G, .)$ je uspořádaná dvojice, sestávající z množiny G (která se též nazývá **nosná množina**) a operace $.$ na G. Rovnost dvou grupoidů znamená tedy jednak rovnost nosných množin a jednak rovnost operací.

Pojem operace na G tak, jak byl výše definován, je možno bez problémů zobecnit na pojem tzv. "n-ární operace" (pro libovolné přirozené n), což je pak jakékoliv zobrazení $G \times G \times \ldots \times G$ (n-krát) $\to G$, tzn. předpis, který každé uspořádané n-tici prvků z G přiřazuje jediný prvek z G. Příkladem n-ární operace na množině $\mathbf{R}$ může být třeba operace $\max(x_1, x_2, \ldots, x_n)$, přiřazující každé uspořádané n-tici reálných čísel to číslo, které je z nich maximální. Pro $n = 1$ (resp. $n = 2$, resp. $n = 3$) se pak užívá názvů unární (resp. binární, resp. ternární) operace. Unární operace na G není tedy nic jiného než libovolné zobrazení $G \to G$ (příkladem unární operace na $\mathbf{N}$ může být "operace přičítání jedničky", která každému přirozenému číslu x přiřadí číslo $x + 1$). Binární operace je pak operací v našem slova smyslu, definovanou výše.

Ve školské matematice i v našem dalším textu se budeme setkávat převážně s operacemi binárními a vyjímečně s unárními. Některé vlastnosti binárních operací lze sice přenést na operace n-ární ($n > 2$), většinou však je toto zobecnění spojeno se značnými obtížemi. Na druhé straně, přenesení vlastností binárních operací na unární operace je buď triviální nebo vůbec nedává smysl. Z těchto důvodů budeme v dalším studovat pouze vlastnosti binárních operací, které pro zjednodušení vyjadřování nazýváme stručně operacemi.

Příklad 1.1.

1. Vezměme množinu celých čísel $\mathbf{Z}$. Pak obyčejné násobení čísel $.$ je zřejmě operací na $\mathbf{Z}$. Tedy $(\mathbf{Z}, .)$ je grupoid. Podobně dostáváme grupoidy $(\mathbf{Z}, +)$, resp. $(\mathbf{Z}, -)$, kde $+$, resp. $-$ značí obvyklé sčítání, resp. odečítání čísel. Je jasné, že se jedná o různé grupoidy, i když nosná množina je ve všech třech případech stejná.

2. Vezmeme-li množinu přirozených čísel $\mathbf{N}$, pak obyčejné odečítání čísel není operací na $\mathbf{N}$ (neboť například $2 - 3 \notin \mathbf{N}$, tzn. nejedná se o zobrazení $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$). Podobně třeba obyčejné dělení čísel není operací na množině $\mathbf{R}$ všech reálných čísel (neboť číslem 0 nelze dělit, tzn. například $1 : 0$ není definováno, a tedy opět se nejedná o zobrazení $\mathbf{R} \times \mathbf{R} \to \mathbf{R}$).

3. Nechť A je libovolná množina. Pak sjednocení, resp. průnik, resp. rozdíl dvou podmnožin množiny A je opět (jednoznačně určená) podmnožina v A. Tedy sjednocení

$\cup$, resp. průnik $\cap$, resp. rozdíl $-$ jsou operace na množině 2^A (tj. na systému všech podmnožin množiny A). Jsou tedy $(2^A, \cup)$, resp. $(2^A, \cap)$, resp. $(2^A, -)$ grupoidy.

4. Nechť A je neprázdná množina. Symbolem A^A označujeme systém všech zobrazení množiny A do množiny A. Pro $f, g \in A^A$ je zřejmě složené zobrazení $g \circ f$ opět zobrazením $A \to A$, tzn. $g \circ f \in A^A$. Je tedy skládání zobrazení $\circ$ operací na množině A^A a $(A^A, \circ)$ je grupoid.

Operace na množině G je tedy, jak bylo výše řečeno, zobrazení $G \times G \to G$, tj. jistý předpis, který každé uspořádané dvojici prvků z G přiřadí jediný prvek z G. Tento předpis je možno zadávat různým způsobem, jak jsme si ukázali již u zobrazení. Pokud je však množina G konečná, pak se ukazuje jako výhodné zadávat operaci na G pomocí tabulky (která se nazývá Cayleyho tabulkou), konstruované takto: do svislého i vodorovného záhlaví tabulky vypisujeme prvky množiny G (ve stejném pořadí). Výsledek operace pro uspořádanou dvojici $(a, b) \in G \times G$ pak zapíšeme do toho políčka tabulky, v němž se protíná řádek označený "a" se sloupcem nadepsaným "b". Použití tabulky při definování operace ukazuje následující příklad.

Příklad 1.2. Nechť $G = \{a, b, c, d\}$; na G definujeme operaci $*$ následující tabulkou:

$*$	a	b	c	d
a	b	a	b	c
b	a	b	c	d
c	b	c	a	c
d	a	d	a	d

Tab. 6

Potom $(G, *)$ je grupoid, při čemž například: $a * d = c$, $d * a = a$, atd.

Definice: Nechť $(G, .)$ je grupoid. Jestliže platí:

(i) $a.(b.c) = (a.b).c$, pro $\forall a, b, c \in G$ (tzv. asociativní zákon)

pak operace $.$ se nazývá **asociativní operace** a $(G, .)$ se nazývá asociativní grupoid neboli **pologrupa**.

(ii) $a.b = b.a$, pro $\forall a, b \in G$ (tzv. komutativní zákon)

pak operace $.$ se nazývá **komutativní operace** a $(G, .)$ se nazývá **komutativní grupoid**.

Příklad 1.3. : Ověříme-li asociativní a komutativní zákon u grupoidů z příkladu 1.1. a 1.2. (proveďte si podrobně sami!), dostáváme, že grupoidy:

$(\mathbf{Z}, .)$, $(\mathbf{Z}, +)$, $(2^A, \cup)$, $(2^A, \cap)$ jsou asociativní i komutativní;

$(\mathbf{Z}, -)$ není asociativní, není komutativní;

$(2^A, -)$ je asociativní i komutativní v případě, že $A = \phi$; jinak není asociativní ani komutativní;

$(A^A, \circ)$ je vždy asociativní (viz V.5.2., kapitoly I.); komutativní je v případě, že A je jednoprvková množina, jinak není;

$(G, *)$ z příkladu 1.2. není asociativní, není komutativní.

Z předchozí definice vyplývá, že v pologrupě součin tří prvků (v daném pořadí) nezáleží na jejich uzávorkování (které u tří prvků lze provést právě dvěma způsoby). Následující věta ukáže, že totéž platí v pologrupě i pro libovolný konečný počet n prvků (kde je počet možných uzávorkování samozřejmě obecně mnohem větší).

Věta 1.1.: *Nechť* $(G, .)$ *je pologrupa; nechť* $a_1, a_2, \ldots, a_n \in G$ $(n \geqslant 2)$. Potom součin prvků $a_1, a_2, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.

[D ů k a z: provedeme matematickou indukcí vzhledem k n.

α) pro $n = 2$ tvrzení triviálně platí

β) předpokládejme, že tvrzení věty platí pro $2, 3, \ldots, n-1$ a dokážeme je pro n. Tedy pro $2 \leqslant k < n$ součin prvků $a_1, a_2, \ldots, a_k$ nezáleží na jejich uzávorkování; označíme jej symbolem $a_1.a_2.\ \ldots\ .a_k$. Nechť a označuje součin prvků $a_1, a_2, \ldots, a_n$ pro jisté uzávorkování. Potom: $a = b.c$, kde b je součinem prvků $a_1, \ldots, a_r$, resp. c je součinem prvků $a_{r+1}, \ldots, a_n$ (kde $r < n$). Podle indukčního předpokladu součin prvků $a_1, \ldots, a_r$ nezáleží na uzávorkování, takže lze psát: $b = a_1.(a_2.\ \ldots\ .a_r)$. Odtud a z definice pologrupy dostáváme:

$$a = b.c = (a_1.(a_2.\ \ldots\ .a_r)).c = a_1.((a_2.\ \ldots\ .a_r).c) = a_1.(a_2.\ \ldots\ .a_n)$$

a výraz napravo již nezávisí na uzávorkování.]

Definice: Nechť $(G, .)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** (nebo též jednička) grupoidu $(G, .)$, jestliže platí:

(1) $\quad a.e = a \ \wedge\ e.a = a$, pro každý prvek $a \in G$.

Z definice není vidět zda, resp. kolik neutrálních prvků v grupoidu může existovat.

Odpověď na tuto otázku nám dává následující věta.

Věta 1.2.: *V grupoidu existuje nejvýše jeden neutrální prvek.*

[D ů k a z: nechť $(G, .)$ je grupoid a nechť $e, e' \in G$ jsou jeho neutrální prvky. Pak platí: $e.e' = e'$ (neboť e je neutrální prvek) a současně $e.e' = e$ (neboť e' je neutrální prvek), odkud plyne: $e' = e$ a věta je dokázána.]

Vidíme tedy, že grupoid má buďto jeden nebo žádný neutrální prvek. V konkretních příkladech postupujeme při hledání neutrálního prvku obvykle tak, že se nejprve snažíme jej "uhádnout" a ověřením (1) dokázat, že se opravdu o neutrální prvek jedná. Toto se nám vetšinou bez problémů podaří (viz příklad 1.4.). U složitějších grupoidů, u nichž nejsme schopni neutrální prvek "uhádnout", je výhodné postupovat způsobem demonstrovaným v příkladech 1.5. a 1.6.

Příklad 1.4.: Vyšetřujeme-li existenci neutrálního prvku u grupoidů z příkladu 1.1. a 1.2., pak lehce zjistíme, že grupoid:
$(\mathbf{Z}, .)$ má neutrální prvek 1; $(\mathbf{Z}, +)$ má neutrální prvek 0;
$(\mathbf{Z}, -)$ nemá neutrální prvek; $(2^A, \cup)$ má neutrální prvek ϕ;
$(2^A, \cap)$ má neutrální prvek A; $(2^A, -)$ má neutrální prvek ϕ v případě, že $A = \phi$, jinak neutrální prvek nemá; $(A^A, \circ)$ má neutrální prvek id_A.
Konečně, grupoid $(G, *)$ z příkladu 1.2. má neutrální prvek b (všimněte si, že v tomto případě grupoid není komutativní a je tedy nutno ověřovat obě rovnosti z (1), zatímco v komutativních grupoidech platí $a.e = e.a$, a stačí tedy ověřovat jenom jednu z rovností (1)).

Příklad 1.5.: Na množině $\mathbf{Z} \times \mathbf{Z}$ definujme operaci $\square$ takto:

$$(a_1, a_2) \square (b_1, b_2) = (a_1 + b_1 + 1,\ a_2 + b_2 - 3), \text{ pro } \forall (a_1, a_2), (b_1, b_2) \in \mathbf{Z} \times \mathbf{Z},$$

kde $+$ značí obyčejné sčítání čísel. Dostáváme tak grupoid $(\mathbf{Z} \times \mathbf{Z}, \square)$ a chceme zjistit, zda má neutrální prvek.

Předpokládejme, že jistá uspořádaná dvojice $(z_1, z_2) \in \mathbf{Z} \times \mathbf{Z}$ je neutrálním prvkem v $(\mathbf{Z} \times \mathbf{Z}, \square)$. Z rovnosti (1) pak buď obdržíme podmínky určující z_1 a z_2, anebo odvodíme spor. V prvním případě jsme nalezli (jediný) neutrální prvek, ve druhém případě pak vyšetřovaný grupoid neutrální prvek nemá. V našem případě stačí ověřovat v (1) jenom jednu z obou rovností (poněvadž operace $\square$ je zřejmě komutativní), tzn.

pro libovolný prvek $(a_1, a_2) \in \mathbf{Z} \times \mathbf{Z}$ musí platit: $(a_1, a_2) \square (z_1, z_2) = (a_1, a_2)$, tzn. $(a_1 + z_1 + 1, a_2 + z_2 - 3) = (a_1, a_2)$. Tedy:

$$a_1 + z_1 + 1 = a_1$$
$$a_2 + z_2 - 3 = a_2$$

odkud dostáváme $z_1 = -1$, $z_2 = 3$. Snadno ověříme, že dvojice $(-1, 3)$ opravdu splňuje (1), tzn. $(-1, 3)$ je neutrálním prvkem grupoidu $(\mathbf{Z} \times \mathbf{Z}, \square)$.

Příklad 1.6. Na množině $\mathbf{Z} \times \mathbf{Z}$ definujeme operaci $\triangle$ takto:

$$(a_1, a_2) \triangle (b_1, b_2) = (a_1 + b_1, a_2), \text{ pro } \forall (a_1, a_2), (b_1, b_2) \in \mathbf{Z} \times \mathbf{Z},$$

kde $+$ značí obyčejné sčítání čísel. Chceme zjistit, zda grupoid $(\mathbf{Z} \times \mathbf{Z}, \triangle)$ má neutrální prvek.

Postupujeme stejně jako v předchozím příkladu. Předpokládejme, že $(z_1, z_2) \in \mathbf{Z} \times \mathbf{Z}$ je neutrálním prvkem. Pak pro libovolný prvek $(a_1, a_2) \in \mathbf{Z} \times \mathbf{Z}$ platí:

$(a_1, a_2) \triangle (z_1, z_2) = (a_1, a_2) \quad \wedge \quad (z_1, z_2) \triangle (a_1, a_2) = (a_1, a_2)$.

Po rozepsání dostáváme čtyři rovnosti: $a_1 + z_1 = a_1$, $a_2 = a_2$, $z_1 + a_1 = a_1$, $z_2 = a_2$, odkud pak: $z_1 = 0 \quad \wedge \quad z_2 = a_2$, což není možné (neboť z_2 nemůže záviset na a_2). Vidíme, že náš předpoklad existence neutrálního prvku vedl ke sporu, a tedy grupoid $(\mathbf{Z} \times \mathbf{Z}, \triangle)$ neutrální prvek nemá.

Poznámka: V dalším budeme místo termínu "neutrální prvek grupoidu $(G, .)$" (tj. při multiplikativní symbolice) používat častěji stručnějšího termínu "jednička grupoidu $(G, .)$".

Pokud budeme používat aditivní symboliku (tj. operaci budeme značit symbolem $+$), pak místo "neutrální prvek grupoidu $(G, +)$" budeme obvykle říkat "nula grupoidu $(G, +)$".

Tato terminologie je motivována situací, kdy při obyčejném násobení (resp. sečítání) čísel hraje roli neutrálního prvku číslo 1 (resp. číslo 0). Stejná motivace bude i při zavádění rozdílných názvů v multiplikativní a aditivní symbolice pro jiné, v dalším definované pojmy.

Definice: Nechť $(G, .)$ je grupoid s jedničkou e; nechť $a \in G$. Pak prvek $x \in G$, pro který platí:

(2) $\qquad a.x = e \quad \wedge \quad x.a = e$

se nazývá **inverzní prvek** k prvku a (v grupoidu $(G, .)$).

Poznámka: 1. používáme-li aditivní symboliku, tzn. máme-li grupoid $(G, +)$ s nulou o, pak místo "inverzní prvek k prvku a" budeme říkat "**opačný prvek** k prvku a". Je to tedy takový prvek $x \in G$, pro nějž platí: $a + x = o \wedge x + a = o$.

2. o počtu inverzních prvků k danému prvku a v grupoidu $(G, .)$ s jedničkou obecně nemůžeme nic říci. Například, v grupoidu $(\mathbf{Z}, .)$ k číslu 3 neexistuje žádný inverzní prvek, zatímco k číslu -1 existuje jediný inverzní prvek (číslo -1). V grupoidu $(G, *)$ z příkladu 1.2. (neutrálním prvkem je zde prvek b) k prvku a existují dva inverzní prvky: a, c. V grupoidu $(\mathbf{Z}, +)$ ke každému prvku existuje jediný opačný prvek, atd.

Pro počet inverzních prvků k danému prvku hraje důležitou roli předpoklad asociativity operace, jak ukazuje následující věta.

Věta 1.3.: *V pologrupě s jedničkou ke každému prvku existuje nejvýše jeden inverzní prvek.*

[D ů k a z: nechť $(G, .)$ je pologrupa s jedničkou e. Nechť $a \in G$ a nechť x, y jsou inverzní prvky k prvku a. Tedy podle definice je:

$$a.x = e, \quad x.a = e, \quad \text{resp.} \quad a.y = e, \quad y.a = e .$$

Potom však: $x = x.e = x.(a.y) = (x.a).y = e.y = y$, odkud dostáváme tvrzení věty.]

Poznámka: 1. z předchozí věty plyne, že když v pologrupě k prvku a existuje prvek inverzní, pak je jediný. V takovém případě budeme tento (jediný) inverzní prvek k prvku a označovat symbolem a^{-1} (při multiplikativní symbolice), resp. symbolem $-a$ (při aditivní symbolice).

2. při hledání inverzních prvků k danému prvku v pologrupě používáme v konkretních případech podobných metod, jakých jsme používali při hledání neutrálního prvku, tj. v jednoduchých situacích se snažíme inverzní prvek "uhádnout" a ověřením (2) dokázat, že jsme "hádali" správně. Pokud se nám to nepodaří, pak podrobným řešením rovností (2) buď inverzní prvek nalezneme, anebo zjistíme, že neexistuje.

Věta 1.4.: *Nechť $(G, .)$ je pologrupa s jedničkou e. Nechť $a, b \in G$ mají v $(G, .)$ inverzní prvky a^{-1}, b^{-1}. Pak platí:*

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

[D ů k a z : 1. a 2. plynou přímo z definice inverzního prvku.

3. rozepsáním dostáváme:

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

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

a tedy prvek $b^{-1}.a^{-1}$ je inverzním prvkem k prvku $a.b$, neboli $b^{-1}.a^{-1} = (a.b)^{-1}$]

Zkusíme-li si rozmyslet a zobecnit naše zkušenosti z počítání s čísly, zjistíme, že se bude zřejmě dobře pracovat s grupoidy, které budou mít několik z výše definovaných vlastností najednou; například budou asociativní, budou mít jedničku a každý jejich prvek bude mít jediný inverzní prvek. Tato úvaha nás vede k následující definici.

Definice: Nechť $(G, .)$ je pologrupa s jedničkou, v níž ke každému prvku existuje prvek inverzní. Pak $(G, .)$ se nazývá **grupa.**

Je-li navíc operace $.$ komutativní, pak se grupa $(G, .)$ nazývá **komutativní grupa** (nebo též abelovská grupa).

Příklad 1.7.:

1. Značí-li $+$ obyčejné sčítání čísel, pak $(\mathbf{Z}, +)$, resp. $(\mathbf{Q}, +)$, resp. $(\mathbf{R}, +)$, resp. $(\mathbf{K}, +)$ jsou komutativní grupy.

2. Nechť $.$ značí obyčejné násobení čísel.

Pak $(\mathbf{Q} - \{0\}, .)$, resp. $(\mathbf{R} - \{0\}, .)$, resp. $(\mathbf{K} - \{0\}, .)$ jsou komutativní grupy.

Nechť $G = \{z \in \mathbf{K} \mid |z| = 1\}$, tj. G je množina všech komplexních čísel ležících na jednotkové kružnici. Pak $(G, .)$ je komutativní grupa (která má zřejmě nekonečně mnoho prvků).

Nechť n je pevné přirozené číslo a nechť $G_n = \{z \in \mathbf{K} \mid z^n = 1\}$, tzn. G je množina všech n-tých odmocnin z jedničky (v oboru komplexních čísel). Pak $(G_n, .)$ je komutativní grupa (ktera má n prvků). Vidíme tedy, že grupa $(G_n, .)$ může sloužit jako příklad komutativní grupy, která má předem pevně daný, konečný počet n prvků.

3. Nechť $A = \{a, b, c\}$; nechť G značí množinu všech bijektivních zobrazení A na A (kterých je celkem 6 - vypište si je!) a nechť $\circ$ značí skládání zobrazení. Pak $(G, \circ)$ je grupa, která není komutativní.

[zřejmě $(G, \circ)$ je grupoid, který podle V.5.2. kapitoly I je asociativní, v němž id_A je neutrálním prvkem a k bijekci f je inverzním prvkem inverzní zobrazení f^{-1}. Tedy $(G, \circ)$ je grupa. Tato grupa není komutativní, neboť jsou-li $f, g \in G$ definovány:

$f(a) = b$, $f(b) = c$, $f(c) = a$, resp. $g(a) = c$, $g(b) = b$, $g(c) = a$, potom: $(f \circ g)(a) = f(c) = a$, ale $(g \circ f)(a) = g(b) = b$, a tedy je $f \circ g \neq g \circ f$].

4. Nechť n je pevné přirozené číslo. Na množině $\mathbf{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbf{R}\}$ definujeme operaci + takto: pro libovolné $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbf{R}^n$ položme:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

kde symboly + na pravé straně značí obyčejné sčítání čísel (poněkud nepřesně, ale výstižně obvykle říkáme, že sčítání uspořádaných n-tic je definováno "po složkách").
Potom $(\mathbf{R}^n, +)$ je komutativní grupa.
[rozepsáním lehce zjistíme, že grupoid $(\mathbf{R}^n, +)$ je asociativní a komutativní, jeho neutrálním prvkem (nulou) je uspořádaná n-tice $(0, 0, \ldots, 0)$ a opačným prvkem k $(a_1, a_2, \ldots, a_n)$ je prvek $(-a_1, -a_2, \ldots, -a_n)$].

Je samozřejmé, že ne každý grupoid nebo pologrupa musí být grupou. Z dříve uvedených grupoidů, resp. pologrup nejsou grupami například:
$(\mathbf{Z}, .)$ - neboť například k 3 neexistuje v $(\mathbf{Z}, .)$ prvek inverzní
$(\mathbf{Z}, -)$ - není asociativní
$(2^A, \cup)$ v případě, že $A \neq \phi$ - pak například k libovolné jednoprvkové podmnožině množiny A neexistuje v $(2^A, \cup)$ prvek inverzní
$(A^A, \circ)$ v případě, že A je alespoň dvouprvková - pak k libovolnému neinjektivnímu zobrazení $A \to A$ neexistuje v $(A^A, \circ)$ prvek inverzní, atd.

Další důležitý příklad komutativní grupy, která má konečný počet prvků, ukazuje následující věta.

Věta 1.5.: *Nechť $\mathbf{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$ je množina zbytkových tříd podle modulu m. Na množině $\mathbf{Z}_m$ definujeme operaci + takto: pro $C_i, C_j \in \mathbf{Z}_m$ libovolné položíme: $C_i + C_j = C_r$, kde*
(3) *r je zbytek po dělení čísla $(i + j)$ číslem m.*
Potom: $(\mathbf{Z}_m, +)$ je komutativní grupa.

Poznámka: je zřejmé, že symbol + ve (3) značí obyčejné sčítání čísel. Dále, z V.3.3. kapitoly I plyne, že podmínku (3) je možné vyslovit dalšími dvěma ekvivalentními způsoby, a sice:

(3') $i + j = z \cdot m + r \quad \wedge \quad 0 \leqslant r \leqslant m - 1$, kde $z \in \mathbf{Z}$

(3'') $i + j \equiv r \pmod{m} \quad \wedge \quad 0 \leqslant r \leqslant m - 1$.

[D ů k a z : 1. $(\mathbf{Z}_m, +)$ je zřejmě grupoid.

2. dokážeme, že operace + je asociativní; nechť tedy $C_i, C_j, C_k \in \mathbf{Z}_m$ jsou libovolné zbytkové třídy. Označme $C_i + C_j = C_r$ a $(C_i + C_j) + C_k = C_s$. Podle (3') pak platí: $i + j = z_1 m + r \quad \wedge \quad 0 \leqslant r \leqslant m - 1$, resp. $r + k = z_2 m + s \quad \wedge \quad 0 \leqslant s \leqslant m - 1$, odkud $r = i + j - z_1 m$ a po dosazení: $i + j - z_1 m + k = z_2 m + s$. Tedy:

(4) $\qquad (i + j + k) = (z_1 + z_2) . m + s \quad \wedge \quad 0 \leqslant s \leqslant m - 1.$

Podobně označme: $C_j + C_k = C_t$ a $C_i + (C_j + C_k) = C_u$. Potom platí: $j + k = z_3 m + t \quad \wedge$ $0 \leqslant t \leqslant m - 1$, resp. $i + t = m_4 k + u \quad \wedge \quad 0 \leqslant u \leqslant m - 1$, odkud po úpravě a dosazení stejně jako výše dostáváme:

(5) $\qquad (i + j + k) = (z_3 + z_4) . m + u \quad \wedge \quad 0 \leqslant u \leqslant m - 1.$

Ale (4) a (5) říká, že jak s, tak u je zbytkem po dělení čísla $(i + j + k)$ číslem m. Podle věty o dělení se zbytkem je však zbytek určen jednoznačně, a tedy $s = u$, neboli $(C_i + C_j) +$ $+ C_k = C_i + (C_j + C_k)$.

3. neutrálním prvkem (nulou) v $(\mathbf{Z}_m, +)$ je třída C_0, neboť ze (3) přímo plyne, že $C_i + C_0 = C_0 + C_i = C_i$, pro libovolné $C_i \in \mathbf{Z}_m$.

4. opačným prvkem k $C_0 \in \mathbf{Z}_m$ je zřejmě opět prvek C_0. Je-li $C_i \in \mathbf{Z}_m$ libovolný prvek, různý od C_0, pak k němu opačný je zřejmě prvek C_{m-i}, neboť $C_{m-i} \in \mathbf{Z}_m$ a platí $C_{m-i} + C_i = C_i + C_{m-i} = C_0$.

5. operace + je komutativní, jak ihned plyne ze (3).]

Pracujeme-li s grupou $(\mathbf{Z}_m, +)$ pro nějaké konkretní m, pak bývá užitečné si sestrojit tabulku operace +. Při tom si zaveďme zjednodušenou symboliku spočívající v tom, že místo symbolu C_i budeme psát pouze symbol i (tzn. místo zbytkové třídy pouze její index). Například pro modul $m = 6$ pak dostáváme:

$m = 6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tab. 7

Upozorňujeme ještě jednou na to, že zde 0 (resp. 1, atd.) je symbol, který je jen jiným označením pro zbytkovou třídu C_0 (resp. C_1, atd.) a neznamená tedy číslo 0 (resp. 1, atd.). Nelze tedy pro tyto symboly používat například pravidla platná pro běžné počítání s čísly.

Definice: Nechť $(G, .)$ je grupoid; řekneme, že

(i) v $(G, .)$ platí **zákony o dělení**, jestliže pro každé $a, b \in G$ platí:

existuje $x \in G$ tak, že $a.x = b$

existuje $y \in G$ tak, že $y.a = b$

(ii) v $(G, .)$ platí **zákony o krácení**, jestliže pro $a, b, x \in G$ libovolné platí:

$x.a = x.b \Rightarrow a = b$

$a.x = b.x \Rightarrow a = b$.

Následující věta ukáže, že v definici grupy lze existenci jedničky a existenci inverzního prvku ke každému prvku nahradit požadavkem platnosti zákonů o dělení.

Věta 1.6.: *Nechť $(G, .)$ je pologrupa. Pak platí: $(G, .)$ je grupa $\Leftrightarrow$ v $(G, .)$ platí zákony o dělení.*

[D ů k a z : "$\Rightarrow$": nechť $(G, .)$ je grupa a nechť $a, b \in G$ libovolné. Položíme-li $x = a^{-1}.b$, resp. $y = b.a^{-1}$ (z definice grupy plyne, že prvek a^{-1} existuje), dostáváme: $a.x = a.(a^{-1}.b) = b$, resp. $y.a = (b.a^{-1}).a = b$. Platí tedy zákony o dělení.

"$\Leftarrow$": nechť v $(G, .)$ platí zákony o dělení. Dokážeme, že:

α) v $(G, .)$ existuje jednička.

Nechť $a \in G$ libovolný; pak $\exists\, e, e' \in G$ tak, že $a.e = a$, resp. $e'.a = a$ (plyne z platnosti zákonů o dělení). Nechť dále $b \in G$ je libovolný prvek. Pak $\exists x, y \in G$ tak, že: $a.x = b$, resp. $y.a = b$ (opět podle zákonů o dělení). Dosazením pak dostáváme:

$$(6)\quad \begin{aligned} b.e &= (y.a).e = y.(a.e) = y.a = b \\ e'.b &= e'.(a.x) = (e'.a).x = a.x = b \end{aligned}$$

Ze (6) dosazením $b = e'$, resp. $b = e$ dostáváme: $e' = e'.e = e$, tzn., že pak opět podle (6) je e jedničkou v $(G, .)$.

β) k libovolnému prvku $a \in G$ existuje prvek inverzní.

Z platnosti zákonů o dělení plyne, že existují $x, y \in G$ tak, že: $a.x = e$, $y.a = e$. Při tom však: $y = y.e = y.(a.x) = (y.a).x = e.x = x$. Tedy x je hledaný inverzní prvek k prvku a.

Dohromady dostáváme, že $(G, .)$ je grupa.]

Věta 1.7.: *Nechť $(G, .)$ je grupa. Pak v $(G, .)$ platí zákony o krácení.*

[D ů k a z : nechť $(G, .)$ je grupa; nechť $a, b, x \in G$ tak, že $x.a = x.b$. Vynásobíme-li tuto rovnost zleva prvkem x^{-1} (který podle předpokladu existuje), dostáváme: $x^{-1}.(x.a) = x^{-1}.(x.b)$, odkud: $a = b$.

Analogicky dokážeme implikaci: $a.x = b.x \Rightarrow a = b$.]

Poznámka: je-li $(G, .)$ pologrupa, pak předchozí větu nelze obrátit, tzn. z platnosti zákonů o krácení obecně neplyne, že $(G, .)$ je grupa. Například v pologrupě $(\mathbf{N}, .)$ přirozených čísel s operací obyčejného násobení čísel platí zákony o krácení, ale zřejmě $(\mathbf{N}, .)$ není grupou.

Definice: Nechť $(G, .)$ je grupa; nechť $a \in G$. Pak **(celočíselná) mocnina prvku** a je definována takto:

$$a^n = \begin{cases} \underbrace{a.a.\ \ldots\ .a}_{n \text{ krát}} & \text{je-li } n \text{ celé kladné číslo} \\ e & \text{je-li } n = 0 \\ \underbrace{a^{-1}.a^{-1}.\ \ldots\ .a^{-1}}_{-n \text{ krát}} & \text{je-li } n \text{ celé záporné číslo} \end{cases}$$

Věta 1.8.: *Nechť $(G, .)$ je grupa; nechť $a \in G$ a nechť m, n jsou libovolná celá čísla. Pak platí:*

1. $a^m.a^n = a^{m+n}$
2. $(a^m)^n = a^{m.n}$

[D ů k a z : I. pro $m > 0$, $n > 0$ nebo $m = 0$, n libovolné celé nebo $n = 0$, m libovolné celé plynou obě tvrzení přímo z předchozí definice.

II. nechť $m < 0$, $n < 0$; potom:

1. $g^m.g^n = \underbrace{(g^{-1}.\ \ldots\ .g^{-1})}_{-m \text{ krát}}.\underbrace{(g^{-1}.\ \ldots\ .g^{-1})}_{-n \text{ krát}} = \underbrace{g^{-1}.\ \ldots\ .g^{-1}}_{(-m-n) \text{ krát}} = g^{m+n}$

2. uvědomme si, že z předchozí definice a z V.1.4.3. (užitím matematické indukce) plyne, že pro libovolné přirozené k je: $g^{-k} = (g^{-1})^k = (g^k)^{-1}$. Užitím tohoto faktu a užitím V.1.4.2. dostáváme:

$(g^m)^n = [(g^{-m})^{-1}]^n = ([(g^{-m})^{-1}]^{-n})^{-1} = ([(g^{-m})^{-n}]^{-1})^{-1} = (g^{-m})^{-n}$.

Ale $m > 0$, $n > 0$, a tedy užitím I. dostáváme:

$(g^{-m})^{-n} = g^{(-m).(-n)} = g^{m.n}$.

III. případ $m < 0$, $n > 0$ a případ $m > 0$, $n < 0$ se dokáží analogickými úvahami jako II.]

Poznámka: používáme-li aditivního zápisu operace, pak místo názvu (celočíselná) mocnina prvku a používáme názvu **(celočíselný)násobek prvku** a, který je tedy definován:

$$n.a = \begin{cases} \underbrace{a + a + \ldots + a}_{n \text{ krát}}, & \text{je-li } n \text{ celé kladné číslo} \\ 0, & \text{je-li } n = 0 \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{-n \text{ krát}}, & \text{je-li } n \text{ celé záporné číslo} \end{cases}$$

V tomto případě mají potom tvrzení předchozí věty formálně tvar:

1. $(m.a) + (n.a) = (m + n) . a$
2. $n . (m.a) = (n.m) . a$

Zde je potřeba dávat obzvláštní pozor na použité symboly, přesněji řečeno na to, že jeden symbol je použit ve dvou různých významech (v 1. znamená symbol + nalevo operaci v dané grupě a napravo sečítání celých čísel; ve 2. značí druhá tečka zprava násobení celých čísel a ostatní tečky značí celočíselný násobek!)

§ 2. Podstruktury struktur s jednou operací.

Definice: Nechť $(G, .)$ je grupoid a nechť H je neprázdná podmnožina množiny G. Řekneme, že podmnožina H je **uzavřená vzhledem k operaci** $.$, jestliže platí:

$a, b \in H$ libovolné $\Rightarrow$ $a.b \in H$.

Poznámka: je-li $(G, .)$ grupoid a podmnožina $H \subseteq G$ je uzavřená vzhledem k operaci $.$, pak můžeme na H zcela přirozeným způsobem definovat operaci, označme ji třeba Δ takto:

pro $a, b \in H$ libovolné položíme: $a \Delta b = a.b$

(chápeme-li operaci jakožto zobrazení, tj. v našem případě $. : G \times G \to G$ a $\Delta : H \times H \to H$, pak vidíme, že Δ je zúžením zobrazení $.$ na množinu $H \times H$).

Dostáváme tak grupoid (H, Δ). Z praktických důvodů zaveďme úmluvu, že operaci Δ na H budeme všude v dalším vždy značit stejným symbolem jako původní operaci na G, tj. symbolem $.$. Máme tedy grupoid $(H, .)$, pro který zavedeme následující pojmenování.

Definice: Nechť $(G, .)$ je grupoid; nechť neprázdná podmnožina $H \subseteq G$ je uzavřená vzhledem k operaci $.$. Pak grupoid $(H, .)$ se nazývá **podgrupoid grupoidu** $(G, .)$.

Věta 2.1.: *Nechť* $(H, .)$ *je podgrupoid grupoidu* $(G, .)$. *Pak platí:*

1. $(G, .)$ *je asociativní* $\Rightarrow$ $(H, .)$ *je asociativní*
2. $(G, .)$ *je komutativní* $\Rightarrow$ $(H, .)$ *je komutativní*
3. *prvek* e *je jednička v* $(G, .)$ $\wedge$ $e \in H$ $\Rightarrow$ e *je jednička v* $(H, .)$.

[D ů k a z : všechna tři tvrzení plynou bezprostředně z definic.]

Poznamenejme, že žádnou z implikací v předchozí větě nelze obecně obrátit. Například v grupoidu $(G, *)$ z příkladu 1.2. je $(\{d\}, *)$ podgrupoidem, který je asociativní, je komutativní a má jedničku d, zatímco celý grupoid $(G, *)$ není asociativní, není komutativní a prvek d není jeho jedničkou.

Definice: Nechť $(G, .)$ je grupa; nechť $(H, .)$ je podgrupoid v $(G, .)$, který je sám grupou. Pak $(H, .)$ se nazývá **podgrupa grupy** $(G, .)$.

Věta 2.2.: *Nechť* $(H, .)$ *je podgrupa grupy* $(G, .)$. *Pak platí:*

1. *jednička podgrupy* $(H, .)$ *je totožná s jedničkou grupy* $(G, .)$
2. *inverzní prvek k prvku* $h \in H$ *v podgrupě* $(H, .)$ *je totožný s inverzním prvkem k prvku* h *v grupě* $(G, .)$.

[D ů k a z : 1. nechť e_H značí jedničku $(H, .)$, resp. e_G značí jedničku $(G, .)$. Pak platí: $e_H . e_H = e_H$ a také $e_H . e_G = e_H$. Tedy $e_H . e_H = e_H . e_G$, odkud užitím zákona o krácení dostáváme, že $e_H = e_G$.

2. nechť x značí inverzní prvek k prvku h v $(H, .)$, resp. y značí inverzi k prvku h v $(G, .)$. Potom je: $h.x = e_H = e_G$, resp. $h.y = e_G$. Tedy $h.x = h.y$ a užitím zákonů o krácení pak $x = y$.]

Poznámka: vzhledem k 2. části předchozí věty nemusíme rozlišovat inverzní prvek k prvku $h \in H$ v podgrupě či v celé grupě. V obou případech budeme používat označení h^{-1}.

Věta 2.3.: *Nechť* $(G, .)$ *je grupa; nechť* H *je neprázdná podmnožina v* G. *Pak následující výroky jsou ekvivalentní:*

(i) $(H, .)$ *je podgrupa grupy* $(G, .)$

(ii) $a, b \in H$ *libovolné* $\Rightarrow$ $a.b \in H \ \wedge \ a^{-1} \in H$

(iii) $a, b \in H$ *libovolné* $\Rightarrow$ $a.b^{-1} \in H$

(iv) $a, b \in H$ *libovolné* $\Rightarrow$ $a^{-1}.b \in H$.

[D ů k a z: "(i) $\Rightarrow$ (ii)" plyne z definice podgrupy

"(ii) $\Rightarrow$ (iii)" zřejmé

"(iii) $\Rightarrow$ (iv)" nechť platí (iii) a nechť $a, b \in H$ libovolné. Pak podle (iii) je: $a.a^{-1} = e \in H$, tzn. $e.a^{-1} = a^{-1} \in H$, resp. $e.b^{-1} = b^{-1} \in H$. Tedy $a^{-1}, b^{-1} \in H$ a opět podle (iii) je: $a^{-1}.b = a^{-1}.(b^{-1})^{-1} \in H$.

"(iv) $\Rightarrow$ (i)" nechť platí (iv); nechť $a, b \in H$ libovolné. Podle (iv) je: $a^{-1}.a = e \in H$, tzn. $a^{-1}.e = a^{-1} \in H$, tzn. $a.b = (a^{-1})^{-1}.b \in H$. Pak $(H, .)$ je podgrupoid v $(G, .)$, který podle V.2.1. (část 1 a 3) je pologrupou s jedničkou, přičemž pro $a \in H$ je $a^{-1} \in H$. Tedy $(H, .)$ je podgrupa grupy $(G, .)$]

Poznámka: předchozí větu často používáme k technickému ověření toho, zda v konkretním případě je $(H, .)$ podgrupou grupy $(G, .)$. Obvykle k tomu používáme část (ii), tzn. ověřujeme, že:

1. $H \subseteq G \ \wedge \ H \neq \phi$
2. $a, b \in H$ libovolné $\Rightarrow$ $a.b \in H$
3. $a \in H$ libovolné $\Rightarrow$ $a^{-1} \in H$.

Příklad 2.1.:

1. Je-li $(G, .)$ libovolná grupa, pak $(\{e\}, .)$ a $(G, .)$ jsou vždycky jejími podgrupami. Tyto podgrupy se nazývají **triviální podgrupy** grupy $(G, .)$. Ostatní podgrupy (pokud existují) se pak nazývají **netriviální podgrupy**.

2. V grupě $(\mathbf{K}, +)$ jsou podgrupami například $(\mathbf{R}, +)$, resp. $(\mathbf{Q}, +)$, resp. $(\mathbf{Z}, +)$ - viz příklad 1.7.1.
Na druhé straně například $(\mathbf{N}, +)$ je podgrupoidem, avšak není podgrupou v $(\mathbf{K}, +)$.

3. V grupě $(\mathbf{R} - \{0\}, .)$ z příkladu 1.7.2. jsou podgrupami například $(\mathbf{Q} - \{0\}, .)$ nebo $(\mathbf{R}^+, .)$, kde $\mathbf{R}^+$ značí množinu všech kladných reálných čísel..

4. V grupě $(\mathbf{K} - \{0\}, .)$ jsou podgrupami například $(\mathbf{R} - \{0\}, .)$ nebo $(G, .)$, kde $G = \{z \in \mathbf{K} \mid |z| = 1\}$ nebo $(G_n, .)$, kde n je pevné přirozené číslo a $G_n = \{z \in \mathbf{K} \mid z^n = 1\}$ (viz příklad 1.7.2). Vidíme tedy, že v grupě, která má nekonečně mnoho prvků mohou existovat jak podgrupy, ktere mají nekonečně mnoho prvků, tak podgrupy, které mají libovolný konečný počet prvků.

Samozřejmě, že v grupě $(\mathbf{K}, +)$, resp. v grupě $(\mathbf{R} - \{0\}, .)$ existuje mnohem více podgrup, než jsme v předchozím příkladu uvedli. Na závěr paragrafu si ukážeme, jak vypadají všechny podgrupy v aditivní grupě celých čísel $(\mathbf{Z}, +)$ a v aditivní grupě zbytkových tříd modulo m $(\mathbf{Z}_m, +)$.

Věta 2.4.: *Mějme grupu $(\mathbf{Z}, +)$; pro libovolné celé nezáporné číslo k označme symbolem $k.\mathbf{Z}$ množinu všech celočíselných násobků čísla k, tzn.*

$$k.\mathbf{Z} = \{n.k \mid n \in \mathbf{Z} \text{ libovolné}\}.$$

Pak platí:

1. *$(k.\mathbf{Z}, +)$ je podgrupou grupy $(\mathbf{Z}, +)$*
2. *všechny podgrupy v $(\mathbf{Z}, +)$ jsou právě grupy $(k.\mathbf{Z}, +)$, pro libovolné $k \geqslant 0$ celé.*

[Důkaz: 1. plyne rozepsáním podle V.2.3. a poznámky za V.1.8.

2. nechť $(H, +)$ je libovolná podgrupa grupy $(\mathbf{Z}, +)$. Jestliže množina H neobsahuje žádné přirozené číslo, musí být $H = \{0\}$, a tedy je $H = 0.\mathbf{Z}$. Nechť tedy H obsahuje nějaké přirozené číslo. Nejmenší přirozené číslo patřící do H označme k. Dokážeme, že potom $H = k.\mathbf{Z}$.

"$\subseteq$" nechť $x \in H$ libovolné; pak (podle věty o dělení se zbytkem) existují $q, r \in \mathbf{Z}$ tak, že: $x = q.k + r \quad \wedge \quad 0 \leqslant r < k$. Ale $x \in H$, $k \in H$, tzn. též $-q.k \in H$, odkud: $x + (-q.k) = r \in H$. Pak ale musí být $r = 0$ (jinak spor s volbou k), a tedy $x = q.k \in k.\mathbf{Z}$.

"$\supseteq$" nechť $x \in k.\mathbf{Z}$ libovolné. Pak je $x = n.k$, kde $n \in \mathbf{Z}$. Ale $k \in H$, a tedy také $n.k = x \in H$.]

Vidíme tedy, že v grupě $(\mathbf{Z}, +)$ existuje nekonečně mnoho podgrup, které musí být výše popsaného tvaru. Specielně: $0.\mathbf{Z} = \{0\}$, $1.\mathbf{Z} = \mathbf{Z}$, $2.\mathbf{Z}$ je množina všech sudých čísel, atd.

Podobným způsobem se dají charakterizovat všechny podgrupy v grupě $(\mathbf{Z}_m, +)$ zbyt-

kových tříd modulo m. Pro libovolné přirozené číslo k, které dělí modul m (tzn. $\frac{m}{k}$ je přirozené číslo) označme:

$$H_k = \{C_{i.k} \mid i = 0, 1, \ldots, \frac{m}{k} - 1\}.$$

Pak lze dokázat, že platí:

1. $(H_k, +)$ je podgrupou grupy $(\mathbf{Z}_m, +)$
2. všechny podgrupy v $(\mathbf{Z}_m, +)$ jsou právě grupy $(H_k, +)$, kde $k \in \mathbf{N} \wedge k \mid m$.

Vidíme tedy, že grupa $(\mathbf{Z}_m, +)$ má právě tolik různých podgrup, kolik přirozených dělitelů má modul m. Vezmeme-li tedy například modul $m = 6$, pak číslo 6 má čtyři přirozené dělitele, a sice 1, 2, 3, 6, a tedy podgrupami v $(\mathbf{Z}_6, +)$ jsou právě $(H_1, +)$, $(H_2, +)$, $(H_3, +)$, $(H_6, +)$, kde $H_1 = \{C_0, C_1, C_2, C_3, C_4, C_5\} = \mathbf{Z}_6$, $H_2 = \{C_0, C_2, C_4\}$, $H_3 = \{C_0, C_3\}$, $H_6 = \{C_0\}$ (pomocí tabulky 7 si sami ověřte, že jde opravdu o podgrupy v $(\mathbf{Z}_6, +)$).

§ 3. Struktury s dvěma operacemi a jejich podstruktury.

V tomto paragrafu se budeme zabývat algebraickými strukturami se dvěma operacemi. Pro tyto dvě operace budeme používat aditivního a multiplikativního způsobu zápisu. Při tom uvidíme, že zaváděné pojmy budou opět do jisté míry zobecňovat vlastnosti běžných struktur se dvěma operacemi, s nimiž jsme se setkali na střední škole, tj. celých, resp. racionálních, resp. reálných čísel s operacemi sečítání čísel a násobení čísel.

Definice: Nechť R je množina se dvěma operacemi $+$ a $.$ taková, že platí:

(i) $(R, +)$ je komutativní grupa

(ii) $(R, .)$ je pologrupa

(iii) pro $\forall a, b, c \in R$ platí: $(a + b) . c = a.c + b.c$
$a . (b + c) = a.b + a.c$ (tzv. distributivní zákony)

Pak R s operacemi $+$ a $.$ se nazývá **okruh** a označuje se $(R, +, .)$.

Poznámka: operaci $+$, resp. $.$ v okruhu $(R, +, .)$ budeme nazývat sečítání, resp. násobení. Neutrální (nulový) prvek grupy $(R, +)$ se nazývá **nula okruhu** $(R, +, .)$ a označuje symbolem 0. Opačný prvek k prvku a v okruhu $(R, +, .)$ budeme označovat symbolem $-a$. Místo: $a + (-b)$ budeme používat stručného zápisu: $a - b$.

Příklad 3.1.:

1. Značí-li +, resp. . obyčejné sčítání, resp. násobení čísel, pak $(\mathbf{Z}, +, .)$, $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$, $(\mathbf{K}, +, .)$, $(\mathbf{S}, +, .)$, $(\mathbf{Z}(\sqrt{2}), +, .)$, $(\mathbf{Q}(\sqrt{2}), +, .)$ jsou okruhy. Při tom $\mathbf{S}$ značí množinu všech sudých celých čísel, resp. $\mathbf{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$, $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$.

2. Na množině $\mathbf{R} \times \mathbf{R}$ definujme operace + a . takto:

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

pro libovolné $(a, b), (c, d) \in \mathbf{R} \times \mathbf{R}$

(kde +, resp. . na pravé straně značí obyčejné sčítání, resp. násobení čísel).
Pak $(\mathbf{R} \times \mathbf{R}, +, .)$ je okruh.

3. Nechť $(R, +)$ je libovolná komutativní grupa; nechť 0 je neutrální prvek této grupy. Definujme na množině R operaci . takto:

pro libovolné $a, b \in R$ položíme: $a.b = 0$.

Pak $(R, +, .)$ je okruh, který se též nazývá **nulový okruh.**

4. Je-li R jednoprvková množina, například $R = \{r\}$, pak na R můžeme definovat operaci jen jedním způsobem. Položíme-li tedy:

$$r + r = r, \quad \text{resp.} \quad r.r = r,$$

pak $(R, +, .)$ je okruh, který se též nazývá **triviální okruh.** Triviální okruh je jakýmsi "patologickým" příkladem okruhu, v němž obě operace splývají, a proto jej často budeme z našich úvah vylučovat.

Věta 3.1.: *Nechť* $\mathbf{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$ je množina zbytkových tříd podle modulu m. Na množině $\mathbf{Z}_m$ definujeme operaci + (stejně jako ve V.1.5.) a . takto: pro $C_i, C_j \in \mathbf{Z}_m$ položme

$C_i + C_j = C_r$, kde r je zbytek po dělení čísla $i + j$ číslem m

$C_i . C_j = C_s$, kde s je zbytek po dělení čísla $i.j$ číslem m.

Pak $(\mathbf{Z}_m, +, .)$ je okruh.

[D ů k a z : 1. $(\mathbf{Z}_m, +)$ je komutativní grupa (viz V.1.5.)

2. $(\mathbf{Z}_m, .)$ je zřejmě grupoid; analogickým způsobem jako ve V.1.5. se ukáže, že operace . je asociativní. Je tedy $(\mathbf{Z}_m, .)$ pologrupou.

3. dokážeme platnost distributivních zákonů; nechť tedy $C_i, C_j, C_k \in \mathbf{Z}_m$ libovolné.

Označme: $(C_i + C_j) = C_r$ a $(C_i + C_j) . C_k = C_s$. Potom platí:

$i + j = z_1 . m + r \quad \wedge \quad 0 \leqslant r < m$, resp. $r . k = z_2 . m + s \quad \wedge \quad 0 \leqslant s < m$,

odkud $r = i + j - z_1 m$ a po dosazení: $(i + j - z_1 m) . k = z_2 . m + s$, tzn.

(1) $\quad i . k + j . k = (z_1 k + z_2) . m + s \quad \wedge \quad 0 \leqslant s < m$

Podobně označme: $C_i . C_k = C_u$; $C_j . C_k = C_v$ a $C_i . C_k + C_j . C_k = C_t$. Potom platí:

$$i . k = z_3 . m + u \quad \wedge \quad 0 \leqslant u < m; \quad j . k = z_4 . m + v \quad \wedge \quad 0 \leqslant v < m,$$

$$u + v = z_5 . m + t \quad \wedge \quad 0 \leqslant t < m,$$

odkud po úpravě a dosazení stejně jako výše dostáváme:

(2) $\quad i . k + j . k = (z_3 + z_4 + z_5) . m + t \quad \wedge \quad 0 \leqslant t < m$

Ale z (1) a (2) užitím věty o dělení se zbytkem dostáváme, že $s = t$, neboli $C_s = C_t$, což znamená, že $(C_i + C_j) . C_k = C_i . C_k + C_j . C_k$.

Druhý z distributivních zákonů plyne ihned z prvního, uvážíme-li, že operace . je zde zřejmě komutativní.]

Pro větší názornost si sestrojme tabulky operací + a . na množině $\mathbf{Z}_m$ pro některá konkretní m, například $m = 6$ a $m = 7$. Při tom stejně jako v § 1 budeme místo symbolu C_i psát pouze i. Potom:

$m = 6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tab. 8a

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tab. 8b

$m = 7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tab. 9a

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tab. 9b

V následujících dvou větách si odvodíme základní pravidla, která platí pro "počítání" v okruhu. Budeme vidět, že jsou podobná pravidlům, která známe ze střední školy pro počítání s čísly.

Věta 3.2.: *Nechť* $(R, +, .)$ *je okruh*; $a, b, c \in R$ *libovolné. Pak platí:*

1. $a \,.\, (b - c) = a.b - a.c \quad ; \quad (b - c) \,.\, a = b.a - c.a$
2. $a.0 = 0.a = 0$
3. $a \,.\, (-b) = (-a) \,.\, b = -(a.b)$
4. $(-a) \,.\, (-b) = a.b$

[D ů k a z : 1. $a \,.\, (b - c) = a \,.\, (b - c) + a.c - a.c = a \,.\, [(b + (-c)) + c] - a.c = a \,.\, [b + (-c + c)] - a.c = a.b - a.c$; zbývající část se dokáže podobně.

2. platí: $a.0 + a.0 = a \,.\, (0 + 0) = a.0 = a.0 + 0$, odkud užitím zákonů o krácení (které v $(R, +)$ platí), dostáváme: $a.0 = 0$. Podobně se ukáže, že $0.a = 0$.

3. Užitím 1. a 2. dostáváme: $a \,.\, (-b) = a \,.\, (0 - b) = a.0 - a.b = 0 - a.b = -a.b$. Podobně se ukáže, že $(-a) \,.\, b = -a.b$.

4. Užitím 3. dostáváme: $(-a) \,.\, (-b) = -((-a) \,.\, b) = -(-a.b) = a.b$]

Věta 3.3.: *Nechť* $(R, +, .)$ *je okruh;* $a, b, a_i, b_j \in R$; z *je celé číslo. Pak platí:*

1. $a \,.\, (a_1 + a_2 + \ldots + a_n) = a.a_1 + a.a_2 + \ldots + a.a_n$
2. $(a_1 + a_2 + \ldots + a_n) \,.\, a = a_1.a + a_2.a + \ldots + a_n.a$
3. $(a_1 + \ldots + a_n) \,.\, (b_1 + \ldots + b_m) = a_1.b_1 + a_1.b_2 + \ldots + a_1.b_m + \ldots + a_n b_1 + \ldots + a_n b_m$
4. $z \,.\, (a.b) = (z.a) \,.\, b = a \,.\, (z.b)$.

[D ů k a z : všechna tvrzení se lehce dokáží užitím matematické indukce. V tvrzení 4 je nutné si uvědomit, že symbol . je zde použit ve dvou významech - jednou pro celočíselný násobek a podruhé pro operaci násobení v okruhu.]

Poznamenejme, že pro zjednodušení zápisu součtu $(a_1 + \ldots + a_n)$ n prvků v okruhu často používáme sumační symboliku, tzn. $\sum_{i=1}^{n} a_i$. První tři tvrzení předchozí věty nám pak udávají jistá pravidla pro práci se sumačními symboly v okruhu, a sice:

1. $a \,.\, \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a.a_i$; 2. $(\sum_{i=1}^{n} a_i) \,.\, a = \sum_{i=1}^{n} a_i.a$; 3. $\sum_{i=1}^{n} a_i \,.\, \sum_{j=1}^{m} b_j = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i.b_j$

Definice: Nechť $(R, +, .)$ je okruh.

Je-li operace $.$ komutativní, pak $(R, +, .)$ se nazývá **komutativní okruh.**

Jestliže pologrupa $(R, .)$ má jedničku, pak tato se nazývá jedničkou okruhu $(R, +, .)$ a označuje se symbolem 1. Okruh $(R, +, .)$ se pak nazývá **okruh s jedničkou.**

Příklad 3.2.:

1. Všechny doposud uvedené příklady okruhů byly komutativní okruhy. Jednoduchý příklad nekomutativního okruhu uvedeme později v kapitole o maticích.

2. Okruhy $(\mathbf{Z}, +, .)$, $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$, $(\mathbf{K}, +, .)$, $(\mathbf{Z}(\sqrt{2}), +, .)$, $(\mathbf{Q}(\sqrt{2}), +, .)$ z příkladu 3.1.1. jsou okruhy s jedničkou. Jedničkou je zde číslo 1.

Okruh $(\mathbf{R} \times \mathbf{R}, +, .)$ z příkladu 3.1.2. je okruhem s jedničkou. Jedničkou je zde uspořádaná dvojice $(1, 1)$.

Okruh zbytkových tříd modulo m $(\mathbf{Z}_m, +, .)$ je okruhem s jedničkou. Jedničkou je zde třída C_1.

3. Okruh sudých čísel $(\mathbf{S}, +, .)$ je okruhem bez jedničky. Rovněž každý netriviální nulový okruh je okruhem bez jedničky.

Definice: Nechť $(R, +, .)$ je okruh; nechť pro nějaké $a, b \in R$ platí:

$$a \neq 0 \quad \wedge \quad b \neq 0 \quad \wedge \quad a.b = 0 .$$

Pak prvky a, b se nazývají **dělitelé nuly** v okruhu $(R, +, .)$.

Netriviální komutativní okruh s jedničkou, který nemá dělitele nuly se nazývá **obor integrity.**

Příklad 3.3.:

1. Klasickým příkladem oboru integrity je okruh celých čísel $(\mathbf{Z}, +, .)$. Dále, okruhy $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$, $(\mathbf{K}, +, .)$, $(\mathbf{Z}(\sqrt{2}), +, .)$, $(\mathbf{Q}(\sqrt{2}), +, .)$ z příkladu 3.1.1. jsou rovněž obory integrity.

2. Okruh $(\mathbf{R} \times \mathbf{R}, +, .)$ z příkladu 3.1.2. není oborem integrity, protože má dělitele nuly (nulou tohoto okruhu je zřejmě $(0, 0)$, přičemž například $(0, 1), (1, 0) \neq (0, 0)$, ale $(0, 1) . (1, 0) = (0, 0)$).

3. Okruh zbytkových tříd modulo 6 $(\mathbf{Z}_6, +, .)$ není oborem integrity, protože má dělitele nuly (nulou je třída C_0, přičemž například $C_2, C_3 \neq C_0$, ale $C_2 . C_3 = C_0$). Na druhé straně, okruh zbytkových tříd modulo 7 $(\mathbf{Z}_7, +, .)$ je oborem integrity (plyne ihned z tabulky 9b). Následující věta nám ukáže, pro která m okruh zbytkových tříd

$(\mathbf{Z}_m, +, .)$ nemá dělitele nuly, tj. je oborem integrity.

Věta 3.4.: *Okruh zbytkových tříd modulo m* $(\mathbf{Z}_m, +, .)$ *je oborem integrity* $\Leftrightarrow$ *m je prvočíslo.*

[D ů k a z : "$\Rightarrow$" nechť $(\mathbf{Z}_m, +, .)$ je obor integrity. Pak je netriviálním okruhem, a tedy musí být $m \geqslant 2$. Dále postupujme sporem; předpokládejme, že m je složené číslo, tzn. existují celá čísla r, s tak, že $1 < r, s < m$ a platí: $r.s = m$. Potom však $C_r, C_s \in \mathbf{Z}_m$, $C_r \neq C_0$, $C_s \neq C_0$ a $C_r . C_s = C_0$, neboli C_r, C_s jsou dělitelé nuly v $(\mathbf{Z}_m, +, .)$, což je spor. Tedy m je prvočíslo.

"$\Leftarrow$" nechť m je prvočíslo. Pak $m \geqslant 2$, tzn. okruh $(\mathbf{Z}_m, +, .)$ je netriviální. Dále je zřejmě komutativním okruhem s jedničkou (viz příklad 3.2). Dokážeme, že $(\mathbf{Z}_m, +, .)$ nemá dělitele nuly: nechť $C_r, C_s \in \mathbf{Z}_m$ tak, že $C_r . C_s = C_0$. Potom z definice operace . plyne, že $m \mid r.s$, odkud podle V.3.5.3., kapitoly I. dostáváme, že $m \mid r$ nebo $m \mid s$. Protože však $0 \leqslant r, s < m$, musí být $r = 0$ nebo $s = 0$. Tedy $(\mathbf{Z}_m, +, .)$ nemá dělitele nuly a dohromady pak dostáváme, že $(\mathbf{Z}_m, +, .)$ je obor integrity.]

Věta 3.5.: *Nechť* $(R, +, .)$ *je okruh;* $a, b, c \in R$. *Pak následující výroky jsou ekvivalentní:*

(i) *okruh* $(R, +, .)$ *nemá dělitele nuly*

(ii) $a.b = a.c \wedge a \neq 0 \Rightarrow b = c$

(iii) $b.a = c.a \wedge a \neq 0 \Rightarrow b = c$.

[D ů k a z: "(i) $\Rightarrow$ (ii)": nechť platí (i) a nechť $a.b = a.c$, $a \neq 0$. Potom $a.b - a.c = 0$, tzn. $a . (b - c) = 0$. Protože $a \neq 0$ a okruh nemá dělitele nuly, musí být $b - c = 0$, neboli $b = c$.

"(ii) $\Rightarrow$ (iii)": nechť platí (ii) a nechť $b.a = c.a$, $a \neq$ o. Potom $(b - c) . a = 0 = (b - c) . 0$. Je-li $(b - c) \neq 0$, pak užitím (ii) dostáváme $a = 0$, což je spor. Je tedy $b - c = 0$, neboli $b = c$.

"(iii) $\Rightarrow$ (i)": provedeme sporem; nechť platí (iii) a nechť okruh $(R, +, .)$ má dělitele nuly, tzn. existují prvky $x, y \in R$, $x \neq 0$, $y \neq 0$, $x.y = 0$. Pak ale: $x.y = 0 = 0.y$, odkud podle (iii) dostáváme $x = 0$, spor. Tedy okruh $(R, +, .)$ nemá dělitele nuly.]

Podmínky (ii) a (iii) z předchozí věty se nazývají **omezené zákony o krácení** (levý a

pravý). Slovo "omezené" zde naznačuje, že nemůžeme krátit všemi prvky z R (v našem případě nelze krátit nulou okruhu).

Definice: Komutativní okruh $(R, +, .)$ s vlastností, že $(R - \{0\}, .)$ je grupa, se nazývá **těleso.**

Uvědomme si několik podstatných faktů, které z definice tělesa bezprostředně vyplývají:

1. Každé těleso musí obsahovat alespoň 2 různé prvky (protože jinak by bylo $R - \{0\} = \phi$, a tedy $(R - \{0\}, .)$ by nemohla být grupou), a sice nulu a jedničku.

2. Ke každému nenulovému prvku v tělese existuje (jediný) inverzní prvek (vzhledem k operaci .).

3. Těleso nemá žádné dělitele nuly (protože množina nenulových prvků je uzavřená vzhledem k operaci . , a tedy součin dvou nenulových prvků musí být opět nenulovým prvkem).

Z toho, co jsme právě řekli, vyplývá, že každé těleso $(R, +, .)$ je oborem integrity. Opak však obecně neplatí (například $(\mathbf{Z}, +, .)$ je obor integrity, který není tělesem). Je-li však množina R konečná, pak opak platí, jak ukazuje následující věta.

Věta 3.6.: *Každý konečný obor integrity je tělesem.*

[D ů k a z : nechť $(R, +, .)$ je konečný obor integrity, tzn. nechť R má n prvků $(n \geqslant 2)$. Zřejmě $(R, +, .)$ je komutativní okruh, tzn. zbývá dokázat, že $(R - \{0\}, .)$ je grupa. Ale $(R - \{0\}, .)$ je pologrupa (zde se využil předpoklad neexistence delitelů nuly!), a tedy podle V.1.6. stačí ukázat, že v $(R - \{0\}, .)$ platí zákony o dělení.

Nejprve uvažme libovolný pevný nenulový prvek $a \in R$. Pak množina $\{a.r \mid r \in R\}$ má n prvků (podle V.3.5. totiž $r_1 \neq r_2 \Rightarrow a.r_1 \neq a.r_2$) a poněvadž je podmnožinou n-prvkové množiny R, musí být:

(3) $\qquad \{a.r \mid r \in R\} = R$.

Nyní, nechť $a, b \in R - \{0\}$ libovolné. Pak ze (3) plyne, že existuje $r \in R$ tak, že $a.r = b$, přičemž zřejmě musí být $r \in R - \{0\}$. Dále je $r.a = b$ (plyne z komutativity operace .), a tedy v $(R - \{0\}, .)$ platí zákony o dělení. Podle V.1.6. je pak $(R - \{0\}, .)$ grupou.]

Příklad 3.4.:

1. $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$, $(\mathbf{K}, +, .)$, $(Q(\sqrt{2}), +, .)$ jsou tělesa. Při tom $+$ a $.$ značí obyčejné sčítání a násobení čísel, resp. $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ (viz příklad 3.1.1.).

2. Na množině $\mathbf{Q} \times \mathbf{Q}$ definujme operace $+$ a $.$ takto:

$$(a, b) + (c, d) = (a + c, \ b + d)$$
$$(a, b) \,.\, (c, d) = (ac - 3bd, \ ad + bc)$$

pro libovolné $(a, b), (c, d) \in \mathbf{Q} \times \mathbf{Q}$

(kde napravo vystupuje obyčejné sčítání, odečítání a násobení čísel).
Pak $(\mathbf{Q} \times \mathbf{Q}, +, .)$ je těleso.

3. Okruh zbytkových tříd $(\mathbf{Z}_m, +, .)$ je tělesem právě tehdy, když modul m je prvočíslo (plyne z V.3.4. a z V.3.6.).

4. Okruhy $(\mathbf{Z}, +, .)$, $(\mathbf{S}, +, .)$ a $(\mathbf{Z}(\sqrt{2}), +, .)$ z příkladu 3.1.1. nejsou tělesa. Podobně okruh $(\mathbf{R} \times \mathbf{R}, +, .)$ z příkladu 3.1.2. není tělesem, resp. nulový okruh není nikdy tělesem a též triviální okruh není tělesem.

Dalším pojmem, kterým se budeme zabývat je pojem tzv. charakteristiky okruhu, resp. tělesa.

Definice: Nechť $(R, +, .)$ je okruh.
Jestliže existuje přirozené číslo k s vlastností:

$$k.x = \underbrace{x + x + \ldots + x}_{k\text{-krát}} = 0 \qquad \text{pro každé } x \in R, \tag{4}$$

pak nejmenší k s vlastností (2) se nazývá **charakteristika okruhu** $(R, +, .)$.
Jestliže žádné přirozené k s vlastností (2) neexistuje, pak řekneme, že okruh $(R, +, .)$ má charakteristiku nula.

Je-li okruh $(R, +, .)$ tělesem, pak totéž říkáme o tělese.

Příklad 3.5.:

1. Okruh $(\mathbf{Z}, +, .)$, resp. tělesa $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$, $(\mathbf{K}, +, .)$ mají charakteristiku 0.
2. Těleso $(\mathbf{Q} \times \mathbf{Q}, +, .)$ z příkladu 3.4.2. má charakteristiku 0.
3. Okruh zbytkových tříd $(\mathbf{Z}_m, +, .)$ má charakteristiku m (tzn. rovnou modulu).
4. Okruh má charakteristiku 1 právě když je triviálním okruhem.

Zjišťujeme-li charakteristiku okruhu podle definice, pak musíme vyšetřovat výraz (2) pro každý prvek $x \in R$, což samozřejmě může být dosti zdlouhavé. Má-li však okruh jedničku, pak se celá situace zjednoduší, neboť pak stačí vyšetřovat výraz (2) pouze pro tuto

jedničku, jak ukáže následující věta.

Věta 3.7.: *Nechť* $(R, +, .)$ *je okruh s jedničkou* 1. *Existuje-li přirozené číslo* k *takové, že* $k.1 = \underbrace{1 + 1 + \ldots + 1}_{k\text{-krát}} = 0$, *pak nejmenší takové* k *je rovno charakteristice okruhu* $(R, +, .)$. *Neexistuje-li takové* k, *pak charakteristika okruhu* $(R, +, .)$ *je nula.*

[D ů k a z: nechť k je nejmenší přirozené číslo s vlastností $k.1 = 0$. Pak pro libovolné $x \in R$ je (užitím V.3.3.4.): $k.x = k . (1.x) = (k.1) . x = 0.x = 0$ a zřejmě k je nejmenší s touto vlastností. Tedy $(R, +, .)$ má charakteristiku k. Zbytek tvrzení plyne z definice charakteristiky.]

Jestliže je daný okruh oborem integrity (což splňuje například každé těleso), pak lze o jeho charakteristice říci ještě více.

Věta 3.8.: *Nechť* $(R, +, .)$ *je obor integrity. Pak platí:*

1. *charakteristika* $(R, +, .)$ *je buď prvočíslo nebo nula*
2. *je-li charakteristika* $(R, +, .)$ *rovna prvočíslu* k, *pak pro lib.* $r \in R$, $r \neq 0$ *jsou*

$$0.r \ , \ 1.r \ , \ 2.r \ , \ \ldots \ , \ (k-1).r$$

navzájem různé prvky a pro libovolné celé číslo z *platí:*

$$z.r = i.r, \quad \text{kde} \quad i \equiv z \pmod{k} \ \wedge \ 0 \leqslant i \leqslant k-1$$

3. *je-li charakteristika* $(R, +, .)$ *rovna nule, pak pro libovolné* $r \in R$, $r \neq 0$ *a libovolná různá celá čísla* z_1, z_2 *je:* $z_1.r \neq z_2.r$.

[D ů k a z : 1. dokážeme sporem; nechť charakteristika $(R, +, .)$ je $k > 0$ a nechť k je složené číslo, tzn. existují přirozená čísla p, q tak, že $1 < p, q < k$ a $p.q = k$. Pak (užitím definice a V.3.3.3.) dostáváme: $0 = k.1 = (p.q) . 1 = (p.1).(q.1)$. Poněvadž $(R, +, .)$ nemá dělitele nuly, je $p.1 = 0$ nebo $q.1 = 0$, spor. Tedy charakteristika k je prvočíslo.

2. nechť $i.r = j.r$, kde $0 \leqslant i, j \leqslant k-1$ a $r \neq 0$. Bez újmy na obecnosti můžeme předpokládat, že $i \leqslant j$. Pak: $0 = j.r - i.r = (j-i) . r = (j-i) . (1.r) = ((j-i) . 1) . r$. Ale $r \neq 0$ a okruh nemá dělitele nuly, tzn. musí být $(j-i) . 1 = 0$. Zřejmě však $0 \leqslant j - i < k$, a tedy z V.3.7. plyne, že $j - i = 0$, neboli $i = j$. Tedy prvky $0.r, 1.r, \ldots, (k-1) . r$ jsou navzájem různé.

Dále, nechť $z \in \mathbf{Z}$ je libovolné. Nechť i značí zbytek po dělení čísla z číslem k. Pak platí: $z = q.k + i$; $0 \leqslant i \leqslant k-1$; $i \equiv z \pmod{k}$ a dále (užitím V.1.8., přepsané do

aditivní symboliky): $z.r = (q.k + i) . r = (q.k) . r + i.r = q . (k.r) + i.r = q . 0 + i.r = i.r$, což dává zbytek tvrzení.

3. dokážeme sporem; nechť $z_1, z_2 \in \mathbf{Z}$ tak, že $z_1 \neq z_2$ a $z_1.r = z_2.r$ (kde $r \neq 0$). Můžeme předpokládat, že $z_1 < z_2$. Potom $(z_2 - z_1) > 0$ a platí: $0 = z_2.r - z_1.r = (z_2 - z_1) . (1.r) = ((z_2 - z_1) . 1) . r$. Ale $(R, +, .)$ nemá dělitele nuly, tzn. musí být $(z_2 - z_1) . 1 = 0$, odtud však podle V.1.7. plyne, že charakteristika $(R, +, .)$ není nula, což je spor. Je tedy $z_1.r \neq z_2.r$.]

Na závěr paragrafu se ještě stručně zmíníme o podstrukturách okruhů a těles.

Definice: Nechť $(R, +, .)$ je okruh; nechť S je neprázdná podmnožina v R, uzavřená vzhledem k operacím + a . . Je-li $(S, +, .)$ okruh (resp. těleso), pak jej nazýváme **podokruh** (resp. **podtěleso**) okruhu $(R, +, .)$.

V případě, že $(R, +, .)$ je těleso, hovoříme o podokruhu tělesa, resp. podtělese tělesa.

Příklad 3.6.: Ukážeme všechny čtyři možnosti, které mohou nastat.

1. Značí-li **S** množinu všech sudých čísel, pak **(S, +, .)** je podokruhem okruhu celých čísel **(Z, +, .)**.

2. Okruh celých čísel **(Z, +, .)** je podokruhem tělesa racionálních čísel **(Q, +, .)**.

3. Nechť **(R × R, +, .)** je okruh z příkladu 3.1.2. a nechť $S = \{(r, 0) \mid r \in \mathbf{R}\}$. Pak $(S, +, .)$ je podtělesem okruhu **(R × R, +, .)**.

4. Těleso racionálních čísel **(Q, +, .)** je podtělesem tělesa reálných čísel **(R, +, .)**.

(Zřejmě + a . v 1., 2., 4. značí obyčejné sčítání a násobení čísel.)

Poznámka: je-li $(S, +, .)$ podokruh okruhu $(R, +, .)$, pak nulové prvky obou okruhů se zřejmě rovnají. Pro jedničky však totéž obecně neplatí - především některý z obou okruhů jedničku vůbec nemusí mít (viz příklad 3.6.1.), a i když oba okruhy jedničku mají, pak obě jedničky mohou být různé (nastane to v případě, že $1_R \notin S$). Například v příkladu 3.6.3. je $1_{\mathbf{R} \times \mathbf{R}} = (1, 1)$, zatímco $1_S = (1, 0)$.

Jestliže je $(S, +, .)$ podtělesem tělesa $(R, +, .)$, pak ovšem $1_S = 1_R$, tzn. obě jedničky splynou (neboť zřejmě $(S - \{0\}, .)$ je podgrupou grupy $(R - \{0\}, .)$).

Následující dvě věty nám pak udávají kriteria pro ověření toho, zda $(S, +, .)$ je podokruhem okruhu, resp. podtělesem tělesa.

Věta 3.9.: *Nechť* $(R, +, .)$ *je okruh; nechť* S *je neprázdná podmnožina množiny* R. *Potom* $(S, +, .)$ *je podokruh okruhu* $(R, +, .)$ *právě když platí:*

(i) $a, b \in S \Rightarrow a - b \in S$

(ii) $a, b \in S \Rightarrow a.b \in S$.

[D ů k a z : tvrzení plyne ihned z definice podokruhu a z V.2.3. (přeformulované do aditivní symboliky).]

Věta 3.10.: *Nechť* $(R, +, .)$ *je těleso; nechť* S *je alespoň dvouprvková podmnožina množiny* R. *Potom* $(S, +, .)$ *je podtělesem tělesa* $(R, +, .)$ *právě když platí:*

(i) $a, b \in S \Rightarrow a - b \in S$

(ii) $a, b \in S \wedge b \neq 0 \Rightarrow a.b^{-1} \in S$.

[D ů k a z : tvrzení opět plyne z definice podtělesa a z V.2.3.]

Na závěr si ještě ukážeme, jak vypadají všechny možné podokruhy v jednom z nejdůležitějších okruhů - v okruhu celých čísel. Poznamenejme, že pro k celé nezáporné jsme symbolem $k.\mathbf{Z}$ označovali množinu všech celých násobků čísla k, tzn. $k.\mathbf{Z} = \{n.k \mid n \in \mathbf{Z}\}$.

Věta 3.11.: *Všechny podokruhy v okruhu celých čísel* $(\mathbf{Z}, +, .)$ *jsou právě okruhy* $(k.\mathbf{Z}, +, .)$ *pro libovolné* $k \geqslant 0$ *celé.*

[D ů k a z: I. pro libovolné $k \geqslant 0$ celé je zřejmě $\phi \neq k.\mathbf{Z} \subseteq \mathbf{Z}$ a podle V.3.9. je $(k.\mathbf{Z}, +, .)$ podokruhem okruhu $(\mathbf{Z}, +, .)$.

II. naopak, nechť $(S, +, .)$ je libovolný podokruh okruhu $(\mathbf{Z}, +, .)$. Pak $(S, +)$ je podgrupou grupy $(\mathbf{Z}, +)$, a tedy užitím V.2.4. dostáváme, že $S = k.\mathbf{Z}$ pro pevné $k \geqslant 0$ celé.]

Podobným způsobem lze pak ukázat, jak vypadají všechny podokruhy v okruhu zbytkových tříd $(\mathbf{Z}_m, +, .)$. Z úvahy za V.2.4. totiž bezprostředně plyne, že podokruhy v $(\mathbf{Z}_m, +, .)$ jsou právě okruhy $(H_k, +, .)$ pro libovolné přirozené k takové, že k dělí m. Při tom symbol H_k označuje množinu:

$$H_k = \{C_{i.k} \mid i = 0, 1, \ldots, \frac{m}{k} - 1\}.$$

Vidíme tedy, že například okruh $(\mathbf{Z}_6, +, .)$ má právě 4 podokruhy, a sice $(H_1, +, .)$, $(H_2, +, .)$, $(H_3, +, .)$ a $(H_6, +, .)$, kde $H_1 = \{C_0, C_1, C_2, C_3, C_4, C_5\} = \mathbf{Z}_6$, $H_2 = \{C_0, C_2, C_4\}$, $H_3 = \{C_0, C_3\}$, $H_6 = \{C_0\}$), z nichž dva jsou podtělesy (a to $(H_2, +, .)$ a $(H_3, +, .)$; ověřte si

sami, že tomu tak je!).

§ 4. Číselná tělesa.

V předchozích paragrafech této kapitoly jsme většinou pracovali s pojmy, které vznikly zobecněním pojmů známých v souvislosti s počítáním s čísly. Jedním z nich byl i pojem tělesa. Typické příklady těles jsme potom podle očekávání nalezli v různých číselných oborech (tzn. mezi podmnožinami množiny **K** všech komplexních čísel), přičemž za operace + a . bylo bráno obyčejné sčítání a obyčejné násobení čísel.

S pojmem tělesa budeme pracovat (samozřejmě kromě celé řady dalších pojmů) ve všech zbývajících kapitolách tohoto textu. Abychom si situaci co nejvíce zjednodušili (při zachování většiny podstatných vlastností), omezíme naše úvahy na tělesa, jejichž prvky budou čísla a operacemi na nich bude obyčejné sčítání a násobení čísel. V tomto paragrafu si shrneme základní vlastnosti takových těles.

Definice: Nechť $(T, +, .)$ je podtělesem tělesa komplexních čísel $(\mathbf{K}, +, .)$. Potom $(T, +, .)$ se nazývá **číselné těleso.**

Poznámka: operacemi v tělese komplexních čísel $(\mathbf{K}, +, .)$ jsou obyčejné sčítání a obyčejné násobení čísel, a tedy i v každém číselném tělese jsou operacemi + a . automaticky obyčejné sčítání a násobení čísel. Proto všude v tomto paragrafu bude +, resp. značit obyčejné sčítání, resp. násobení čísel. Dále poznamenejme, že ve smyslu dříve zavedených úmluv bude $a - b$ znamenat obyčejný rozdíl čísel a, b, resp. $\frac{a}{b}$ bude znamenat obyčejný podíl čísel a, b $(b \neq 0)$.

Praktické zjišťování, zda $(T, +, .)$ je číselným tělesem, provádíme pomocí následující věty.

Věta 4.1.: *Nechť T je podmnožina v* **K**, *obsahující více než jeden prvek. Potom* $(T, +, .)$ *je číselným tělesem právě když platí:*

(i) $a, b \in T \Rightarrow a - b \in T$

(ii) $a, b \in T \wedge b \neq 0 \Rightarrow \frac{a}{b} \in T$.

[D ů k a z : Věta je doslovným přepisem V.3.10., a proto platí.]

Příklad 4.1.:

1. $(\mathbf{Q}, +, .)$, $(\mathbf{R}, +, .)$, $(\mathbf{K}, +, .)$ jsou zřejmě číselnými tělesy.

2. Označme $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$. Potom $(\mathbf{Q}(\sqrt{2}), +, .)$ je číselné těleso.

[důkaz: (použijeme předchozí větu); zřejmě $\mathbf{Q}(\sqrt{2})$ obsahuje více než jeden prvek. Dále, nechť $a + b\sqrt{2}$, $c + d\sqrt{2} \in \mathbf{Q}(\sqrt{2})$, tzn. $a, b, c, d \in \mathbf{Q}$. Potom

(i) $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbf{Q}(\sqrt{2})$, protože zřejmě $(a - c), (b - d) \in \mathbf{Q}$.

(ii) nechť navíc $c + d\sqrt{2} \neq 0$; potom též $c - d\sqrt{2} \neq 0$ a platí:

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2} \cdot \sqrt{2} \in \mathbf{Q}(\sqrt{2}),$$

protože oba zlomky jsou zřejmě racionálními čísly.

Podle V.4.1. je tedy $(\mathbf{Q}(\sqrt{2}), +, .)$ číselným tělesem.]

3. Při stejném označení lze stejným způsobem ukázat, že $(\mathbf{Q}(\sqrt{3}), +, .)$, $(\mathbf{Q}(\sqrt{5}), +, .)$, $(\mathbf{Q}(\sqrt{7}), +, .)$, ..., $(\mathbf{Q}(\sqrt{p}), +, .)$ (kde p je libovolné prvočíslo), jsou číselná tělesa.

4. Označme $\mathbf{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbf{Q}\}$. Potom $(\mathbf{Q}(\sqrt[3]{2}), +, .)$ je číselné těleso (což se ukáže podobným výpočtem jako u 2.).

5. Při stejném označení lze stejným způsobem ukázat, že $(\mathbf{Q}(\sqrt[3]{3}), +, .)$, $(\mathbf{Q}(\sqrt[3]{5}), +, .)$, ... jsou číselná tělesa.

6. Označme $\mathbf{Q}(i) = \{a + bi \mid a, b \in \mathbf{Q}\}$. Potom $(\mathbf{Q}(i), +, .)$ je číselné těleso, což se ukáže opět obdobným výpočtem jako u 2. části tohoto příkladu.

Z předchozích příkladů vidíme především, že číselných těles je rozhodně nekonečně mnoho, a dále, že číselná tělesa se neomezují pouze na reálnou osu (viz příklad 4.1.6.).

Rozebereme-li předchozí příklady, zjistíme, že všechna uvedená číselná tělesa obsahovala těleso racionálních čísel. Že tomu tak musí být vždycky (tzn., že tedy těleso racionálních čísel je nejmenším číselným tělesem), ukazuje 1. část následující věty.

Věta 4.2.: *Nechť $(T, +, .)$ je libovolné číselné těleso. Potom platí:*

1. $(T, +, .)$ obsahuje těleso racionálních čísel (tzn. $T \supseteq \mathbf{Q}$)

2. $(T, +, .)$ má charakteristiku nula.

[D ů k a z: 1. z definice tělesa plyne, že musí existovat prvek $a \in T$, $a \neq 0$. Potom $\frac{a}{a} = 1 \in T$, tzn. T obsahuje číslo 1. Sečteme-li jedničku se sebou samou libovolný konečný počet-krát, pak výsledek opět musí ležet v T, a tedy T obsahuje množinu všech

přirozených čísel.

Dále: $a - a = 0 \in T$, resp. pro libovolné přirozené číslo $n \in T$ je $-n = 0 - n \in T$, a tedy T obsahuje všechna záporná čísla. Dohromady pak $\mathbf{Z} \subseteq T$.

Konečně v T leží i podíl libovolných dvou celých čísel (s nenulovým jmenovatelem), tzn. každé racionální číslo. Dostáváme tak: $\mathbf{Q} \subseteq T$.

2. plyne ihned z V.3.7.]

Pro úplnost připomeňme, že 1. část předchozí věty obecně nelze obrátit, tzn. jestliže $M \supseteq \mathbf{Q}$, pak $(M, +, .)$ obecně nemusí být číselným tělesem. Například, je-li $M = \mathbf{Q} \cup \{\sqrt{2}\}$, pak zřejmě $M \supseteq \mathbf{Q}$, ale $(M, +, .)$ není číselným tělesem (neboť $\sqrt{2} \in M$, ale $\sqrt{2} + \sqrt{2} = 2\sqrt{2} \notin M$).

III. VEKTOROVÉ PROSTORY

§1 : Vektorový prostor nad číselným tělesem

Pojem vektoru a vektorového prostoru je jedním ze základních pojmů moderní matematiky, kterého se využívá nejenom v řadě disciplin ryzí matematiky, ale rovněž v mnoha aplikacích, ať už v přírodních vědách nebo jinde.

Při zavádění pojmu vektorového prostoru se oproti předchozí kapitole situace poněkud komplikuje v tom, že tentokrát vycházíme ze dvou algebraických struktur, a to z jisté komutativní grupy $(V, +)$, jejíž prvky budeme označovat tučnými písmeny, a dále z jistého číselného tělesa $(T, +, .)$. Mezi těmito dvěma strukturami pak budou platit určité vazby. Pro zjednodušení vyjadřování si zaveďme následující úmluvu.

Úmluva: při zapisování algebraických struktur už nebudeme vždy důsledně vypisovat symboly operací jako doposud, ale často budeme k označení celé struktury používat pouze symbol nosné množiny.

Tedy např. místo o grupě $(V, +)$ budeme stručně hovořit o grupě V, místo o tělese $(T, +, .)$ budeme stručně hovořit o tělese T, atd. Při tom je však třeba mít stále na paměti, že se jedná o zjednodušené označení, protože, jak víme, algebraickou strukturu nelze ztotožňovat pouze s její nosnou množinou.

Definice: Nechť $(V, +)$ je komutativní grupa (jejíž prvky nazýváme vektory) a $(T, +, .)$ je číselné těleso. Nechť pro každé číslo $t \in T$ a každý vektor $\mathbf{u} \in V$ je definován vektor $t.\mathbf{u} \in V$ tak, že platí:

(i) $t \,.\, (\mathbf{u} + \mathbf{v}) = t.\mathbf{u} + t.\mathbf{v}$

(ii) $(t + s) \,.\, \mathbf{u} = t.\mathbf{u} + s.\mathbf{u}$ pro lib. $t, s \in T$ a $\mathbf{u},\mathbf{v} \in V$

(iii) $(t.s) \,.\, \mathbf{u} = t \,.\, (s \,.\, \mathbf{u})$

(iv) $1 \,.\, \mathbf{u} = \mathbf{u}$

Potom V se nazývá **vektorový prostor nad tělesem** T.

Označení: Nulový prvek z $(V, +)$ se nazývá **nulový vektor** a označuje se symbolem $\mathbf{o}$. Opačný prvek k vektoru $\mathbf{u} \in V$ se nazývá **opačný vektor k vektoru** $\mathbf{u}$ a označuje se symbolem $-\mathbf{u}$. Vektor $t.\mathbf{u}$ se nazývá **součin čísla** t **s vektorem** $\mathbf{u}$.

Poznámka: výše definovaný součin čísla s vektorem je vlastně speciálním typem zobraze-

ní, a sice zobrazením $T \times V \to V$, které se někdy nazývá vnější operace, na rozdíl od (binární) operace na množině, např. V, což je zobrazení $V \times V \to V$, které se pak nazývá vnitřní operace.

V definici vektorového prostoru se setkáváme se třemi vnitřními operacemi a jednou vnější operací, při čemž některé z nich označujeme stejnými symboly (sčítání ve V a sčítání v T symbolem $+$, resp. násobení v T a součin čísla s vektorem symbolem $.$). I když nemůže dojít k nedorozumění (vzhledem k tomu, že vektory z V a čísla z T odlišujeme graficky), je třeba si tuto skutečnost dobře uvědomit.

Připomeňme, že máme-li korektně definovat nějaký konkretní vektorový prostor, pak z předchozí definice plyne, že musíme:

1. zadat číselné těleso T
2. zadat množinu vektorů V
3. zadat, jak je definováno sčítání vektorů
4. zadat, jak je definován součin čísla z T s vektorem z V
5. ověřit, že $(V, +)$ je komutativní grupa a že platí axiomy (i) - (iv) z definice vektorového prostoru.

Příklad 1.1.

1. Nechť T je libovolné číselné těleso, n je pevné přirozené číslo a nechť:

$$T^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in T\}$$

(tzn. T^n je množina všech uspořádaných n-tic prvků z tělesa T) je množina vektorů. Definujme pro lib. $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{v} = (v_1, \ldots, v_n) \in T^n$ a $t \in T$:

$$\mathbf{u} + \mathbf{v} = (u_1 + v_1, \ldots, u_n + v_n), \qquad t.\mathbf{u} = (t.u_1, \ldots, t.u_n)$$

kde symboly $+$, resp. $.$ na pravých stranách značí obyčejné sčítání, resp. násobení čísel (stručně říkáme, že sčítání vektorů a násobení čísla s vektorem je definováno "po složkách"). Pak $(T^n, +)$ je komutativní grupa (viz příklad 1.7.4, kap. II) a lehce se ověří, že platí axiomy (i) - (iv) z definice vektorového prostoru.

Tedy T^n je vektorovým prostorem nad tělesem T.

Poznamenejme, že nulovým vektorem je v T^n zřejmě uspořádaná n-tice $(0,0, \ldots, 0)$ a opačným vektorem k $(u_1, \ldots, u_n)$ je vektor $(-u_1, \ldots, -u_n)$.

Specielně, např. $\mathbf{R}^3$, $\mathbf{Q}^5$, $\mathbf{K}^2$, $\mathbf{Q}(\sqrt{2})^4$, atd. jsou různé vektorové prostory tohoto typu.

2. Vezměme těleso $\mathbf{R}$ reálných čísel; množinou vektorů bude množina všech polynomů o neurčité x, s reálnými koeficienty, kterou označme $\mathbf{R}[x]$. Sčítání vektorů definujeme jako obvyklé sčítání polynomů a součin čísla s vektorem definujeme jako obvyklé násobení polynomu reálným číslem.

Lehce se ověří, že $(\mathbf{R}[x], +)$ je komutativní grupa a že platí axiomy (i) - (iv).

Tedy $\mathbf{R}[x]$ je vektorovým prostorem nad tělesem $\mathbf{R}$.

(Nulovým vektorem tohoto vektorového prostoru je pak zřejmě tzv. nulový polynom, tj. polynom, jehož všechny koeficienty jsou nulové).

3. Nechť n je pevné přirozené číslo; vezměme opět těleso $\mathbf{R}$ reálných čísel a množinou vektorů nechť je množina sestávající z nulového polynomu a dále ze všech polynomů o neurčité x, s reálnými koeficienty, stupně $\leqslant n$, kterou označíme symbolem $\mathbf{R}_n[x]$. Tedy:

$$\mathbf{R}_n[x] = \{a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \mid a_0, a_1, \ldots, a_n \in \mathbf{R}\} .$$

Sčítání vektorů a součin čísla s vektorem definujeme stejně jako v předchozím příkladu.

Lehce se ověří, že $(\mathbf{R}_n[x], +)$ je komutativní grupa a že platí axiomy (i) - (iv).

Tedy $\mathbf{R}_n[x]$ je vektorovým prostorem nad tělesem $\mathbf{R}$.

4. Nechť T je libovolné číselné těleso a $V = \{\mathbf{v}\}$ je libovolná jednoprvková množina. Sčítání vektorů a součin čísla s vektorem definujeme (jediným možným způsobem, a sice): $\mathbf{v} + \mathbf{v} = \mathbf{v}$, resp. $t.\mathbf{v} = \mathbf{v}$, pro každé $t \in T$. Pak zřejmě $(V, +)$ je komutativní grupa a platí axiomy (i) - (iv). Tedy V je vektorový prostor nad tělesem T, který budeme nazývat **nulový vektorový prostor** (nad T). Je to tedy vektorový prostor, obsahující jediný vektor - a to nulový, tzn. $\mathbf{v} = \mathbf{o}$.

Poznámka: Uvědomme si, že množina vektorů V je vždy neprázdná, dále, že nulový vektor ve V existuje jediný a opačný vektor k libovolnému vektoru z V existuje rovněž jediný (to vše plyne ihned z faktu, že $(V, +)$ je grupa). Při tom je potřeba důsledně rozlišovat symboly $\mathbf{o}$ a 0, tzn. nulový vektor a číslo nula.

Dále připomeňme, že podle dříve zavedené úmluvy budeme místo $\mathbf{u} + (-\mathbf{v})$ psát stručně $\mathbf{u} - \mathbf{v}$. Následující věta nám pak dá další pravidla pro počítání s vektory.

Věta 1.1.: *Nechť V je vektorový prostor nad tělesem T; nechť $t,s \in T$, $\mathbf{u}, \mathbf{v} \in V$ lib. Pak platí:*

1. $t \,.\, (\mathbf{u} - \mathbf{v}) = t.\mathbf{u} - t.\mathbf{v}$
2. $(t - s) \,.\, \mathbf{u} = t.\mathbf{u} - s.\mathbf{u}$

3. $t.\mathbf{u} = \mathbf{o} \Leftrightarrow t = 0$ nebo $\mathbf{u} = \mathbf{o}$

4. $t.(-\mathbf{u}) = (-t).\mathbf{u} = -(t.\mathbf{u})$

[D ů k a z: provedeme většinou užitím axiomů (i) - (iv) vektorového prostoru.

1. $t . (\mathbf{u} - \mathbf{v}) = t . (\mathbf{u} + (-\mathbf{v})) + t.\mathbf{v} - t.\mathbf{v} = t . (\mathbf{u} + (-\mathbf{v}) + \mathbf{v}) - t.\mathbf{v} = t.\mathbf{u} - t.\mathbf{v}$

2. $(t - s) . \mathbf{u} = (t + (-s)) . \mathbf{u} + s.\mathbf{u} - s.\mathbf{u} = (t + (-s) + s) . \mathbf{u} - s.\mathbf{u} = t.\mathbf{u} - s.\mathbf{u}$

3. "⇐": je-li $t = 0$, pak $0.\mathbf{u} = (0 - 0).\mathbf{u} = 0.\mathbf{u} - 0.\mathbf{u} = \mathbf{o}$, podle 2.;

je-li $\mathbf{u} = \mathbf{o}$, pak $t.\mathbf{o} = t.(\mathbf{o} - \mathbf{o}) = t.\mathbf{o} - t.\mathbf{o} = \mathbf{o}$, podle 1.

"⇒": nechť $t.\mathbf{u} = \mathbf{o}$ a $t \neq 0$. Potom $\mathbf{u} = 1.\mathbf{u} = (\frac{1}{t} . t).\mathbf{u} = \frac{1}{t} . (t.\mathbf{u}) = \frac{1}{t} . \mathbf{o} = \mathbf{o}$

4. plyne z 1.2 a 3., a sice: $t.(-\mathbf{u}) = t.(\mathbf{o} - \mathbf{u}) = t.\mathbf{o} - t.\mathbf{u} = \mathbf{o} - t.\mathbf{u} = -t.\mathbf{u}$, resp.

$(-t).\mathbf{u} = (0 - t).\mathbf{u} = 0.\mathbf{u} - t.\mathbf{u} = -t.\mathbf{u}$]

Poznámka: pomocí předchozí věty můžeme upřesnit naši představu o počtu vektorů ve vektorovém prostoru. Je-li totiž V libovolný vektorový prostor nad T, různý od nulového prostoru (jinými slovy řečeno - V obsahuje alespoň jeden nenulový vektor), pak musí prostor V obsahovat nekonečně mnoho vektorů. Vezmeme-li totiž libovolný vektor $\mathbf{u} \in V$, $\mathbf{u} \neq \mathbf{o}$ a tvoříme součiny všech prvků z číselného tělesa T (kterých je nekonečně mnoho) s tímto vektorem $\mathbf{u}$, dostáváme nekonečně mnoho navzájem různých vektorů (je-li totiž $t_1.\mathbf{u} = t_2.\mathbf{u}$, pro $t_1, t_2 \in T$, pak $(t_1 - t_2).\mathbf{u} = \mathbf{o}$, odkud podle V.1.1.3. je $(t_1 - t_2) = 0$, neboli $t_1 = t_2$).

§2. Podprostory vektorového prostoru.

Definice: Nechť V je vektorový prostor nad tělesem T. Neprázdná podmnožina W množiny V se nazývá **podprostor vektorového prostoru** V, jestliže platí:

(i) $\mathbf{u}, \mathbf{v} \in W$ libovolné $\Rightarrow \mathbf{u} + \mathbf{v} \in W$

(ii) $t \in T$, $\mathbf{u} \in W$ libovolné $\Rightarrow t.\mathbf{u} \in W$.

Poznámka: 1. lehce se dá ověřit, (proveďte si podrobně sami!), že podmínky (i) a (ii) z předchozí definice jsou ekvivalentní následující jediné podmínce:

(iii) $\mathbf{u}, \mathbf{v} \in W$; $t, s \in T$ libovolné $\Rightarrow t.\mathbf{u} + s.\mathbf{v} \in W$

2. Každý podprostor W vektorového prostoru V musí vždycky obsahovat nulový vektor [je-li $\mathbf{u} \in W$ libovolný, pak podle (ii) a podle V.1.1.3 je $0.\mathbf{u} = \mathbf{o} \in W$]. Vidíme tedy, že se např. nemůže stát, aby dva podprostory vektorového prostoru V byly disjunktní.

Věta 2.1.: *Nechť W je podprostor vektorového prostoru V nad tělesem T. Pak W je sám vektorovým prostorem nad tělesem T.*

[D ů k a z: součet dvou vektorů z W, resp. součin čísla z T s vektorem z W jsou definovány stejně jako ve V. Definice podprostoru nám zaručuje, že jde o vnitřní, resp. vnější operaci na W.

Dále, nechť $\mathbf{u}, \mathbf{v} \in W$ lib.; pak $(-1).\mathbf{v} = -\mathbf{v} \in W$ a tedy $\mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v}) \in W$ (podle V.1.1.4 a definice podprostoru). Podle V.2.3., kap. II je pak $(W, +)$ podgrupou komutativní grupy $(V, +)$, tzn. $(W, +)$ je komutativní grupou.

Axiomy (i) - (iv) z definice vektorového prostoru jsou ve W zřejmě splněny (poněvadž jsou splněny v celém V).

Tedy W je vektorový prostor nad tělesem T.]

Příklad 2.1.:

1. Nechť V je libovolný vektorový prostor nad tělesem T. Pak zřejmě $W = \{\mathbf{o}\}$ a $W = V$ jsou vždy podprostory ve V. Tyto dva podprostory se nazývají **triviální podprostory** ve V. Všechny ostatní podprostory ve V (pokud existují) se pak nazývají **netriviální podprostory** ve V.

2. Uvažme vektorový prostor $\mathbf{R}^3$ (viz příklad 1.1.1). Potom např.:

   a) $W_1 = \{(x, y, 0) \mid x, y \in \mathbf{R} \text{ lib.}\}$ je podprostor vektorového prostoru $\mathbf{R}^3$

   b) $W_2 = \{(x, y, z) \mid x, y, z \in \mathbf{R} \wedge x - 2y + 3z = 0\}$ je podprostor v $\mathbf{R}^3$

   c) nechť (u, v, w) je pevný vektor prostoru $\mathbf{R}^3$; potom $W_3 = \{k \,.\, (u, v, w) \mid k \in \mathbf{R}\}$ je podprostor v $\mathbf{R}^3$.

Je vidět, že vektorový prostor $\mathbf{R}^3$ obsahuje nekonečně mnoho podprostorů. Na druhé straně samozřejmě ne každá podmnožina v $\mathbf{R}^3$ je podprostorem $\mathbf{R}^3$. Např. $W_4 = \{(x, y, 1) \mid x, y \in \mathbf{R}\}$ není podprostorem v $\mathbf{R}^3$ (zdůvodněte proč!).

3. Uvažme vektorový prostor $\mathbf{R}[x]$ všech polynomů (viz příklad 1.1.2). Pak např.:

   a) $W_1 = \{f(x) \in \mathbf{R}[x] \mid f(x) = f(-x)\}$ je podprostorem v $\mathbf{R}[x]$

   b) $W_2 = \{f(x) \in \mathbf{R}[x] \mid 2.f(0) + 3.f(1) = 0\}$ je podprostorem v $\mathbf{R}[x]$

   c) vektorový prostor $\mathbf{R}_n[x]$ (viz příklad 1.1.3) je podprostorem v $\mathbf{R}[x]$.

   Na druhé straně např. množina $W_3 = \{x^2 + ax + b \mid a, b \in \mathbf{R} \text{ lib.}\}$ není podprostorem v $\mathbf{R}[x]$.

Věta 2.2. *Nechť V je vektorový prostor nad tělesem T; nechť I je neprázdná*

indexová množina a nechť pro každé $\alpha \in I$ *je* W_α *podprostor ve* V. *Potom* $\bigcap_{\alpha \in I} W_\alpha$ *je podprostor ve* V.

[D ů k a z: množina $\bigcap_{\alpha \in I} W_\alpha$ je zřejmě neprázdná (neboť obsahuje jistě nulový vektor o). Zbývá tedy ověřit platnost podmínek (i) a (ii) z definice podprostoru: nechť $\mathbf{u}, \mathbf{v} \in \bigcap_{\alpha \in I} W_\alpha$, $t \in T$ libovolné. Potom $\mathbf{u}, \mathbf{v} \in W_\alpha$ pro každé $\alpha \in I$, a tedy (poněvadž W_α je podprostor) je $\mathbf{u} + \mathbf{v} \in W_\alpha$ a $t.\mathbf{u} \in W_\alpha$, pro každé $\alpha \in I$. Pak ale $\mathbf{u} + \mathbf{v} \in \bigcap_{\alpha \in I} W_\alpha$ a $t.\mathbf{u} \in \bigcap_{\alpha \in I} W_\alpha$]

Poznamenejme, že indexová množina I byla libovolná (neprázdná), a tedy předchozí věta platí jak pro konečný, tak pro nekonečný počet podprostorů. Stručně řečeno, věta tvrdí, že průnikem libovolného počtu podprostorů ve V je opět podprostor ve V. Tohoto faktu využijeme v následující důležité úvaze.

Nechť M je libovolná podmnožina vektorového prostoru V (tzn. M obecně není podprostorem!). Pak existuje alespoň jeden podprostor, obsahující množinu M (např. celý prostor V má tuto vlastnost). Můžeme tedy utvořit průnik všech podprostorů ve V, obsahujících množinu M, který označme symbolem $[M]$. Tedy

(1) $$[M] = \cap W_\alpha \quad (W_\alpha \text{ je podprostor ve } V \text{ takový, že } W_\alpha \supseteq M)$$

a platí následující tvrzení:

Věta 2.3. *Nechť* M *je libovolná podmnožina ve vektorovém prostoru* V. *Potom:*

1. $[M]$ *je podprostor ve* V

2. $[M]$ *je nejmenší (vzhledem k* $\subseteq$*) podprostor ve* V, *obsahující množinu* M.

[D ů k a z: 1: plyne ihned z V.2.2.

2: plyne z (1) a ze základních vlastností množinového průniku.]

Je-li množina M konečná, např. $M = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$, pak místo symbolu $[\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}]$ budeme psát stručněji $[\mathbf{u}_1, \ldots, \mathbf{u}_k]$. V tomto případě je tedy

$$[\mathbf{u}_1, \ldots, \mathbf{u}_k] = \cap W_\alpha \quad (W_\alpha \text{ je podprostor ve } V \text{ takový, že } \mathbf{u}_1, \ldots, \mathbf{u}_k \in W_\alpha)$$

Může se samozřejmě též stát, že množina M je prázdná; v takovém případě zřejmě je $[\phi] = \{\mathbf{o}\}$.

Definice. Nechť M je podmnožina ve vektorovém prostoru V a nechť $W = [M]$.

Pak podprostor W se nazývá **podprostor generovaný množinou** M.

Je-li specielně $M = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$, pak W se nazývá **podprostor generovaný vektory** $\mathbf{u}_1, \ldots, \mathbf{u}_k$ a vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ se nazývají **generátory podprostoru** W.

Uvědomme si, že na rozdíl od průniku podprostorů, není množinové sjednocení podprostorů (dokonce ani dvou) obecně podprostorem daného vektorového prostoru. Například pro podprostory W_1 a W_2 vektorového prostoru $\mathbf{R}^3$ z příkladu 2.1.2., jejich sjednocení $W_1 \cup W_2$ není podprostorem v $\mathbf{R}^3$ (neboť např. $(1,1,0), (1,2,1) \in W_1 \cup W_2$, ale $(1,1,0) + (1,2,1) = (2,3,1) \notin W_1 \cup W_2$). V dalším si nyní zavedeme pojem tzv. součtu podprostorů, ukážeme, že je podprostorem a jaký má vztah k množinovému sjednocení těchto podprostorů.

Definice. Nechť $W_1, W_2, \ldots, W_k$ $(k \geq 2)$ jsou podprostory vektorového prostoru V. Pak množina $W_1 + W_2 + \ldots + W_k$ definovaná:

$$W_1 + W_2 + \ldots + W_k = \{\mathbf{u}_1 + \mathbf{u}_2 + \ldots + \mathbf{u}_k \mid \mathbf{u}_1 \in W_1, \mathbf{u}_2 \in W_2, \ldots, \mathbf{u}_k \in W_k\}$$

se nazývá **součet podprostorů** $W_1, \ldots, W_k$.

Věta 2.4. *Nechť $W_1, W_2, \ldots, W_k$ $(k \geq 2)$ jsou podprostory ve V. Pak platí:*

1. součet podprostorů $W_1 + W_2 + \ldots + W_k$ je podprostorem ve V.

2. $W_1 + W_2 + \ldots + W_k = [W_1 \cup W_2 \cup \ldots \cup W_k]$, tzn. součet podprostorů $W_1, \ldots, W_k$ je roven podprostoru generovanému jejich množinovým sjednocením.

[Důkaz: 1: zřejmě je $W_1 + \ldots + W_k \neq \phi$ (neboť $W_i \neq \phi$). Dále, nechť $\mathbf{u}, \mathbf{v} \in W_1 + \ldots + W_k$, $t \in T$ libovolné. Potom $\mathbf{u} = \mathbf{u}_1 + \ldots + \mathbf{u}_k$, $\mathbf{v} = \mathbf{v}_1 + \ldots + \mathbf{v}_k$, kde $\mathbf{u}_i, \mathbf{v}_i \in W_i$, $i = 1, \ldots, k$. Potom ale:

$$\mathbf{u} + \mathbf{v} = (\mathbf{u}_1 + \ldots + \mathbf{u}_k) + (\mathbf{v}_1 + \ldots + \mathbf{v}_k) =$$
$$= (\mathbf{u}_1 + \mathbf{v}_1) + \ldots + (\mathbf{u}_k + \mathbf{v}_k) \in W_1 + \ldots + W_k$$
$$t.\mathbf{u} = t \,.\, (\mathbf{u}_1 + \ldots + \mathbf{u}_k) = t.\mathbf{u}_1 + \ldots + t.\mathbf{u}_k \in W_1 + \ldots + W_k \,,$$

a tedy $W_1 + \ldots + W_k$ je podprostor ve V.

2: vzhledem k (1) budeme dokazovat množinovou rovnost:

$$W_1 + \ldots + W_k = \cap U_\alpha \quad (U_\alpha \text{ je podprostor ve } V \text{ takový, že } U_\alpha \supseteq W_1 \cup \ldots \cup W_k)$$

"$\subseteq$": nechť $\mathbf{u} \in W_1 + \ldots + W_k$, potom $\mathbf{u} = \mathbf{u}_1 + \ldots + \mathbf{u}_k$, kde $\mathbf{u}_i \in W_i$. Je tedy $\mathbf{u}_i \in U_\alpha$, kde U_α je libovolný podprostor ve V takový, že $U_\alpha \supseteq W_1 \cup \ldots \cup W_k$. Potom však $\mathbf{u}_1 + \ldots + \mathbf{u}_k = \mathbf{u} \in U_\alpha$, a tedy $\mathbf{u} \in \cap U_\alpha$ (U_α je podprostor ve V a $U_\alpha \supseteq W_1 \cup \ldots \cup W_k$).

"$\supset$": zřejmě je $W_i \subseteq W_1 + \ldots + W_k$ (neboť pro $\mathbf{u}_i \in W_i$ libovolný je $\mathbf{u}_i = \mathbf{o} + \ldots + \mathbf{u}_i + \ldots + \mathbf{o} \in W_1 + \ldots + W_k$), a tedy $W_1 \cup \ldots \cup W_k \subseteq W_1 + \ldots + W_k$. Podle 1. části věty je však $W_1 + \ldots + W_k$ podprostorem ve V, tzn. z vlastností množinového průniku pak již plyne žádaná množinová inkluse.]

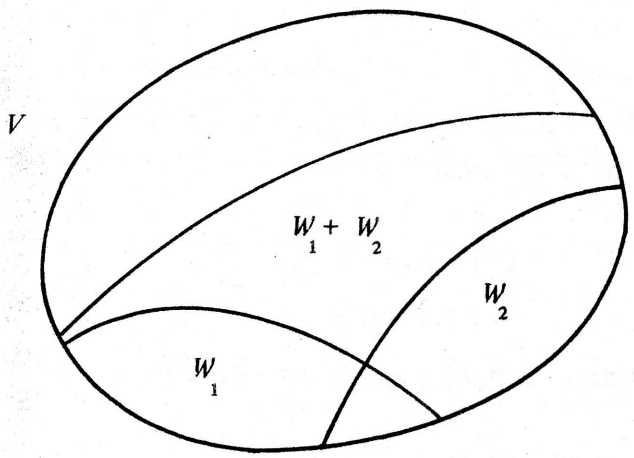
Vidíme tedy, že součet podprostorů $W_1 + \ldots + W_k$ je nejmenším podprostorem ve V, obsahujícím množinové sjednocení $W_1 \cup \ldots \cup W_k$ těchto podprostorů. Samozřejmě, že součet podprostorů obecně není roven jejich množinovému sjednocení. Dále si uvědomme, že vyjádření vektoru $\mathbf{u} \in W_1 + \ldots + W_k$ ve tvaru

$$\mathbf{u} = \mathbf{u}_1 + \ldots + \mathbf{u}_k, \text{ kde } \mathbf{u}_1 \in W_1, \ldots, \mathbf{u}_k \in W_k$$

nemusí být jednoznačné. Obojí si ukážeme na jednoduchém příkladu, a to pro $k = 2$, což je situace, s níž se budeme v praxi nejčastěji setkávat. V tomto případě je tedy

$$W_1 + W_2 = \{\mathbf{u}_1 + \mathbf{u}_2 \mid \mathbf{u}_1 \in W_1, \mathbf{u}_2 \in W_2\} = [W_1 \cup W_2]$$

Schematicky je tato situace znázorněna na obr. 8.



Obr. 8

Příklad 2.2.: Ve vektorovém prostoru $\mathbf{R}^3$ mějme dány dva podprostory:

$$W_1 = \{(x, y, 0) \mid x, y \in \mathbf{R}\}\,; \qquad W_2 = \{(u, 0, v) \mid u, v \in \mathbf{R}\}\,.$$

Zřejmě platí, že:

$$W_1 \cup W_2 = \{(a, b, c) \mid a, b, c \in \mathbf{R},\ b = 0 \text{ nebo } c = 0\}, \text{ resp. } W_1 + W_2 = \mathbf{R}^3$$

Vidíme tedy, že $W_1 \cup W_2 \subsetneq W_1 + W_2$.

Dále, vyjádření vektoru $\mathbf{u} \in W_1 + W_2$ ve tvaru

$$\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2, \quad \text{kde } \mathbf{u}_1 \in W_1, \mathbf{u}_2 \in W_2 \tag{2}$$

zde obecně není jednoznačné, neboť např. $(0,0,0) \in W_1 + W_2$, přičemž třeba $(0,0,0) = (0,0,0) + (0,0,0) = (1,0,0) + (-1,0,0)$ jsou dvě různá vyjádření tvaru (2). Poznamenejme, že v tomto případě má každý vektor z $W_1 + W_2$ dokonce nekonečně mnoho různých vyjádření tvaru (2).

Definice. Nechť $W_1, W_2, \ldots, W_k$ $(k \geqslant 2)$ jsou podprostory vektorového prostoru V. Součet podprostorů $W_1, \ldots, W_k$ se nazývá **přímý součet** a označuje $W_1 \dot{+} W_2 \dot{+} \ldots \dot{+} W_k$, jestliže libovolný vektor $\mathbf{u} \in W_1 + \ldots + W_k$ lze vyjádřit jediným způsobem ve tvaru:

$$\mathbf{u} = \mathbf{u}_1 + \ldots + \mathbf{u}_k\,, \quad \text{kde } \mathbf{u}_1 \in W_1, \ldots, \mathbf{u}_k \in W_k \tag{3}$$

Věta 2.5.: *Nechť $W_1, W_2, \ldots, W_k$ $(k \geqslant 2)$ jsou podprostory vektorového prostoru V. Pak součet podprostorů $W_1, \ldots, W_k$ je přímým součtem $\Leftrightarrow$ pro každé $i = 1, 2, \ldots, k$ platí:*

$$W_i \cap (W_1 + \ldots + W_{i-1} + W_{i+1} + \ldots + W_k) = \{\mathbf{o}\}\,. \tag{4}$$

[D ů k a z: "$\Rightarrow$" nechť součet podprostorů $W_1, \ldots, W_k$ je přímý a nechť pro $1 \leqslant i \leqslant k$ je $\mathbf{x} \in W_i \cap (W_1 + \ldots + W_{i-1} + W_{i+1} + \ldots + W_k)$ libovolný. Potom je $\mathbf{x} = \mathbf{u}_1 + \ldots + \mathbf{u}_{i-1} + \mathbf{u}_{i+1} + \ldots + \mathbf{u}_k$, kde $\mathbf{u}_j \in W_j$, a dále $\mathbf{x} \in W_i$, tzn. také $-\mathbf{x} \in W_i$. Pak ale:

$$\mathbf{o} = \mathbf{u}_1 + \ldots + \mathbf{u}_{i-1} + (-\mathbf{x}) + \mathbf{u}_{i+1} + \ldots + \mathbf{u}_k, \text{ resp. } \mathbf{o} = \mathbf{o} + \mathbf{o} + \ldots + \mathbf{o}$$

jsou dvě vyjádření nulového vektoru $\mathbf{o}$ ve tvaru (3), tzn. podle předpokladu musí být $\mathbf{x} = \mathbf{o}$. Tedy je $W_i \cap (W_1 + \ldots + W_{i-1} + W_{i+1} + \ldots + W_k) \subseteq \{\mathbf{o}\}$. Opačná inkluse

je však triviální, tzn. dohromady platí rovnost. Poněvadž i bylo libovolné (s vlastností $1 \leqslant i \leqslant k$), platí všechny podmínky (4).

"$\Leftarrow$" nechť platí podmínky (4); nechť $\mathbf{x} \in V$ libovolný a nechť

$$\mathbf{x} = \mathbf{u}_1 + \ldots + \mathbf{u}_k = \mathbf{u}'_1 + \ldots + \mathbf{u}'_k, \quad \text{kde } \mathbf{u}_i, \mathbf{u}'_i \in W_i, \quad i = 1,2, \ldots, k$$

jsou dvě vyjádření vektoru $\mathbf{x}$ ve tvaru (3). Potom pro libovolné $i = 1,2, \ldots, k$ dostáváme: $(\mathbf{u}_i - \mathbf{u}'_i) = (\mathbf{u}'_1 - \mathbf{u}_1) + \ldots + (\mathbf{u}'_{i-1} - \mathbf{u}_{i-1}) + (\mathbf{u}'_{i+1} - \mathbf{u}_{i+1}) + \ldots + (\mathbf{u}'_k - \mathbf{u}_k)$, tzn.

$$(\mathbf{u}_i - \mathbf{u}'_i) \in W_i \cap (W_1 + \ldots + W_{i-1} + W_{i+1} + \ldots + W_k)$$

odkud však podle (4) plyne, že $(\mathbf{u}_i - \mathbf{u}'_i) = \mathbf{o}$, neboli $\mathbf{u}_i = \mathbf{u}'_i$. Tedy vyjádření vektoru $\mathbf{x}$ ve tvaru (3) je jednoznačné a součet podprostorů $W_1, \ldots, W_k$ je přímý.]

Poznámka: rozepíšeme-li si předchozí větu pro některá konkretní k, pak dostáváme např.:

pro $k = 2$:

součet podprostorů W_1, W_2 *je přímým součtem* $\Leftrightarrow$ $W_1 \cap W_2 = \{\mathbf{o}\}$

pro $k = 3$:

součet podprostorů W_1, W_2, W_3 *je přímým součtem* $\Leftrightarrow$ $W_1 \cap (W_2 + W_3) = \{\mathbf{o}\} \wedge$ $\wedge\ W_2 \cap (W_1 + W_3) = \{\mathbf{o}\} \wedge W_3 \cap (W_1 + W_2) = \{\mathbf{o}\}$

Příklad 2.3. Ve vektorovém prostoru $\mathbf{R}^3$ mějme dány podprostory:

$$W_1 = \{(x,x,0) | x \in \mathbf{R}\}, \quad W_2 = \{(u,0,v) | u, v \in \mathbf{R}\}, \quad W_3 = \{(0,k,k) | k \in \mathbf{R}\}$$

Potom užitím V.2.5. dostáváme, že

a) součet podprostorů W_1, W_2 je přímý [je-li $\mathbf{w} \in W_1 \cap W_2$, pak $\mathbf{w} = (x, x, 0) =$ $= (u,0,v) \Rightarrow x = 0$, tzn. $\mathbf{w} = (0,0,0)$ a podle V.2.5. je součet přímý]

b) součet podprostorů W_1, W_3 je přímý

c) součet podprostorů W_2, W_3 je přímý

d) součet podprostorů W_1, W_2, W_3 není přímý [neboť např. $W_1 \cap (W_2 + W_3) =$ $= W_1 \cap \mathbf{R}^3 = W_1 \neq \{\mathbf{o}\}$, a tedy podle V.2.5. součet není přímý].

§3: Lineární závislost a nezávislost vektorů

Definice: Nechť V je vektorový prostor nad T; nechť $\mathbf{u}_1, \ldots, \mathbf{u}_k$ je konečná

posloupnost vektorů z V. Pak vektor

$$\mathbf{u} = t_1.\mathbf{u}_1 + \ldots + t_k.\mathbf{u}_k, \quad \text{kde } t_1, \ldots, t_k \in T$$

se nazývá lineární kombinace konečné posloupnosti vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_k$ nebo stručně **lineární kombinace vektorů** $\mathbf{u}_1, \ldots, \mathbf{u}_k$

Množina všech lineárních kombinací vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_k$ se bude označovat symbolem $L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$, tzn.

$$L(\mathbf{u}_1, \ldots, \mathbf{u}_k) = \{t_1.\mathbf{u}_1 + \ldots + t_k.\mathbf{u}_k \mid t_1, \ldots, t_k \in T \text{ libovolné}\}$$

Poznámka: 1. všimněme si, že v předchozí definici hovoříme o "konečné posloupnosti vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_k$". Tímto obratem chceme říci, že je možné, aby se zde některý z vektorů vyskytoval případně vícekrát (tzn. může se stát, že $\mathbf{u}_i = \mathbf{u}_j$, pro $i \neq j$) a dále, že vektory chápeme v uvedeném pořadí (tento fakt však bude hrát důležitou roli až v dalším paragrafu). Z důvodů stručnosti budeme však v dalším místo "konečná posloupnost vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_k$" říkat obvykle pouze "vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$".

2. Symbol $L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ znamená množinu všech (možných) lineárních kombinací vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_k$, kterých je zřejmě obecně nekonečně mnoho. Uvědomme si dále, že množina $L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ obsahuje vždy mimo jiné:

- každý z vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_k$ (neboť $\mathbf{u}_i = 0.\mathbf{u}_1 + \ldots + 0.\mathbf{u}_{i-1} + 1.\mathbf{u}_i + 0.\mathbf{u}_{i+1} + \ldots + 0.\mathbf{u}_k$)
- nulový vektor (neboť $\mathbf{o} = 0.\mathbf{u}_1 + \ldots + 0.\mathbf{u}_k$).

3. V předchozím paragrafu jsme hovořili o podprostoru generovaném konečnou množinou vektorů. Je zřejmé, že místo "konečné množiny vektorů" můžeme vzít též "konečnou posloupnost vektorů" (případné opakující se vektory zde nehrají žádnou roli) a použít stejnou symboliku. Je-li tedy $\mathbf{u}_1, \ldots, \mathbf{u}_k$ konečná posloupnost vektorů z V, pak

(1) $[\mathbf{u}_1, \ldots, \mathbf{u}_k] = \cap W_\alpha$ (W_α je podprostor ve V takový, že $\mathbf{u}_1, \ldots, \mathbf{u}_k \in W_\alpha$) je **podprostor generovaný vektory** $\mathbf{u}_1, \ldots, \mathbf{u}_k$. Následující věta nám pak ukáže, že $[\mathbf{u}_1, \ldots, \mathbf{u}_k]$ a $L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ jsou vlastně jedno a totéž.

Věta 3.1. *Nechť V je vektorový prostor nad T; nechť $\mathbf{u}_1, \ldots, \mathbf{u}_k$ je konečná posloupnost vektorů z V. Pak platí:*

1. $L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ je podprostor ve V

2. $[\mathbf{u}_1, \ldots, \mathbf{u}_k] = L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$, *tzn. podprostor generovaný vektory* $\mathbf{u}_1, \ldots, \mathbf{u}_k$ *je roven množině všech lineárních kombinací vektorů* $\mathbf{u}_1, \ldots, \mathbf{u}_k$.

[D ů k a z: 1. zřejmé (ověřením definice podprostoru)

2. vzhledem k (1) budeme dokazovat množinovou rovnost:

(2) $\cap W_\alpha$ (W_α je podprostor ve $V \wedge \mathbf{u}_1, \ldots, \mathbf{u}_k \in W_\alpha$) $= L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$.

"$\subseteq$" plyne z vlastností množinového průniku, uvědomíme-li si, že $L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ je podprostor ve V (podle 1. části) a že $\mathbf{u}_1, \ldots, \mathbf{u}_k \in L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$

"$\supseteq$" množina na levé straně (2) je podprostor ve V, obsahující vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$, tzn. musí pak obsahovat také jejich libovolnou lineární kombinaci.]

Důsledek: *Nechť* V *je vektorový prostor nad* T, *nechť* $\mathbf{u}_1, \ldots, \mathbf{u}_k$ *je konečná posloupnost vektorů z* V *a nechť* $\mathbf{v}_1, \ldots, \mathbf{v}_s \in L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$. *Pak platí:*

1. $L(\mathbf{v}_1, \ldots, \mathbf{v}_s) \subseteq L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$ *(neboli* $[\mathbf{v}_1, \ldots, \mathbf{v}_s] \subseteq [\mathbf{u}_1, \ldots, \mathbf{u}_k]$)
2. $[\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{v}_1, \ldots, \mathbf{v}_s] = [\mathbf{u}_1, \ldots, \mathbf{u}_k]$

[D ů k a z: 1. plyne ihned z (1) a z předchozí věty, část 2.

2. inkluse "$\supseteq$" plyne z (1);dokažme inklusi "$\subseteq$". Ale triviálně je $\mathbf{u}_1, \ldots, \mathbf{u}_k \in L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$, resp. podle předpokladu je $\mathbf{v}_1, \ldots, \mathbf{v}_s \in L(\mathbf{u}_1, \ldots, \mathbf{u}_k)$. Podle části 1. je pak $[\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{v}_1, \ldots, \mathbf{v}_s] \subseteq [\mathbf{u}_1, \ldots, \mathbf{u}_k]$. Dohromady pak platí dokazovaná rovnost.]

Vidíme tedy, že přidáme-li ke generátorům daného podprostoru W libovolný vektor, který je jejich lineární kombinací, dostáváme opět generátory W, resp. (totéž - jinak řečeno) odstraníme-li z generátorů podprostoru W vektor, který je lineární kombinací zbývajících, dostáváme opět generátory W.

Příklad 3.1.

1. Rozepsáním se lehce ověří, že např.

$\mathbf{R}^2 = [(1,0), (0,1)] = [(1,1), (1,2)] = [(0,2), (1,1), (0,1)] = [(1,3), (2,1), (1,-1), (-2,3)]$, atd. Vidíme tedy, že vektorový prostor $\mathbf{R}^2$ je možno generovat dvěma a více vektory (zřejmě i nekonečně mnoha). Na druhé straně, prostor $\mathbf{R}^2$ evidentně nelze generovat jedním vektorem (neboť $[(a, b)] = L((a, b)) = \{(k.a, k.b) \mid k \in \mathbf{R}\} \subsetneq \mathbf{R}^2$).

2. Ve vektorovém prostoru T^n označme vektory:

$\mathbf{e}_1 = (1,0, \ldots, 0)$, $\mathbf{e}_2 = (0,1,0, \ldots, 0)$, $\ldots$, $\mathbf{e}_n = (0, \ldots, 0,1)$.

Pak platí, že $T^n = [\mathbf{e}_1, \ldots, \mathbf{e}_n]$, tzn. vektory $\mathbf{e}_1, \ldots, \mathbf{e}_n$ jsou generátory vektorového prostoru T^n (zřejmě pro libovolný vektor $\mathbf{u} = (u_1, \ldots, u_n) \in T^n$ je $\mathbf{u} = u_1.\mathbf{e}_1 + \ldots + u_n.\mathbf{e}_n$, tzn. $T^n \subseteq [\mathbf{e}_1, \ldots, \mathbf{e}_n]$ a opačná inkluse je triviální).

3. Ve vektorovém prostoru $\mathbf{R}_n[x]$ označme vektory (tj. polynomy):

$$\mathbf{f}_1 = 1 \quad , \quad \mathbf{f}_2 = x \quad , \quad \mathbf{f}_3 = x^2 \quad , \ldots , \quad \mathbf{f}_{n+1} = x^n \ .$$

Pak zřejmě $\mathbf{R}_n[x] = [\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_{n+1}]$, tzn. polynomy $1, x, x^2, \ldots, x^n$ jsou generátory vektorového prostoru $\mathbf{R}_n[x]$.

Definice: Nechť V je vektorový prostor nad T a nechť

(3) $\qquad \mathbf{u}_1, \ldots, \mathbf{u}_k$

je konečná posloupnost vektorů z V. Jestliže existují čísla $t_1, \ldots, t_k \in T$, z nichž alespoň jedno je různé od nuly, tak, že

(4) $\qquad t_1.\mathbf{u}_1 + \ldots + t_k.\mathbf{u}_k = \mathbf{o}$

pak říkáme, že **vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně závislé.**

V opačném případě říkáme, že **vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně nezávislé.**

Poznámka: vidíme, že pojem lineární nezávislosti je negací pojmu lineární závislosti. Explicitně vyjádřeno to znamená:

" vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně nezávislé, jestliže pro všechna $t_1, \ldots, t_k \in T$, z nichž alespoň jedno je různé od nuly, platí $t_1.\mathbf{u}_1 + \ldots + t_k.\mathbf{u}_k \neq \mathbf{o}$"

S touto definicí by se však zřejmě nešikovně pracovalo, a proto ji přeformulujeme do ekvivalentního, ale praktičtějšího tvaru:

"vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně nezávislé, jestliže platí:

$$t_1.\mathbf{u}_1 + \ldots + t_k.\mathbf{u}_k = \mathbf{o} \ \Rightarrow \ t_1 = t_2 = \ldots = t_k = 0"$$

Praktické zjišťování závislosti či nezávislosti daných vektorů (3) provádíme obvykle tak, že hledáme všechna čísla $t_1, \ldots, t_k \in T$, splňující rovnost (4). Zjistíme-li, že (4) je splněno pouze pro $t_1 = \ldots = t_k = 0$, pak jsou vektory (3) lineárně nezávislé. Je-li rovnost (4) splněna i pro nějaké $t_i \neq 0$, pak jsou dané vektory lineárně závislé.

Příklad 3.2.

1. Ve vektorovém prostoru $\mathbf{R}^2$ jsou např. vektory (1,0), (0,1) lineárně nezávislé; podobně vektory (1,1), (1,2) jsou též lineárně nezávislé (obojí dostaneme rozepsáním podle předchozího návodu).

Na druhé straně např. vektory (0,2), (1,1), (0,1) jsou lineárně závislé a podobně vektory (1,3), (2,1), (1,−1), (−2,3) jsou též lineárně závislé (ověřte si sami!).

2. Ve vektorovém prostoru T^n jsou vektory $\mathbf{e}_1 = (1,0,\ldots,0)$, $\mathbf{e}_2 = (0,1,0,\ldots,0)$, ..., $\mathbf{e}_n = (0,\ldots,0,1)$ lineárně nezávislé (neboť, je-li $t_1.\mathbf{e}_1 + \ldots + t_n.\mathbf{e}_n = (0,\ldots,0)$, pak $(t_1,\ldots,t_n) = (0,\ldots,0)$, a tedy $t_1 = t_2 = \ldots = t_n = 0$).

3. Ve vektorovém prostoru $\mathbf{R}_n[x]$ jsou vektory (polynomy) $\mathbf{f}_1 = 1$, $\mathbf{f}_2 = x$, ..., $\mathbf{f}_{n+1} = x^n$ lineárně nezávislé (je-li $t_1.1 + t_2.x + \ldots + t_{n+1}.x^n = o$, kde o značí nulový polynom, tj. polynom, jehož všechny koeficienty jsou rovny nule, potom je $t_1 = t_2 = \ldots = t_n = 0$, neboť dva polynomy se rovnají právě když se rovnají jejich koeficienty u stejných mocnin x).

Jestliže uvažovaná posloupnost vektorů obsahuje pouze jediný vektor, např. $\mathbf{u}$, pak je zjišťování lineární závislosti či nezávislosti velmi jednoduché, neboť z předchozí definice a z V.1.1.3. plyne (rozmyslete si podrobně jak!), že platí:

(5) *vektor* $\mathbf{u}$ *je lineárně závislý* $\Leftrightarrow$ $\mathbf{u} = \mathbf{o}$

O trošku složitější je situace, když uvažovaná posloupnost (3) obsahuje alespoň dva vektory. Kriteria lineární závislosti nám pro tento případ udává následující věta.

Věta 3.2. *Nechť V je vektorový prostor nad T, nechť $k \geqslant 2$ a $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in V$ Pak následující výroky jsou ekvivalentní:*

(i) *vektory* $\mathbf{u}_1, \ldots, \mathbf{u}_k$ *jsou lineárně závislé*

(ii) $\exists\, i$ $(1 \leqslant i \leqslant k)$ *tak, že vektor* $\mathbf{u}_i$ *je lineární kombinací zbývajících vektorů (tj. vektorů* $\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}, \mathbf{u}_{i+1}, \ldots, \mathbf{u}_k$)

(iii) $\exists\, i$ $(1 \leqslant i \leqslant k)$ *tak, že* $[\mathbf{u}_1, \ldots, \mathbf{u}_k] = [\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}, \mathbf{u}_{i+1}, \ldots, \mathbf{u}_k]$

[D ů k a z: "(i) ⇒ (ii)" nechť $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně závislé. Pak existují čísla $t_1, \ldots, t_k \in T$, z nichž alespoň jedno je nenulové, tak, že $t_1.\mathbf{u}_1 + \ldots + t_k.\mathbf{u}_k = \mathbf{o}$. Nechť např. $t_i \neq 0$. Pak ale úpravou z předchozí rovnice dostáváme:

$$\mathbf{u}_i = -\frac{t_1}{t_i}\mathbf{u}_1 - \ldots - \frac{t_{i-1}}{t_i}\mathbf{u}_{i-1} - \frac{t_{i+1}}{t_i}\mathbf{u}_{i+1} - \ldots - \frac{t_k}{t_i}\mathbf{u}_k$$

což znamená, že vektor $\mathbf{u}_i$ je lineární kombinací zbývajících vektorů.

"(ii) ⇒ (iii)" plyne přímo z 2. části důsledku V.3.1.

"(iii) ⇒ (i)" nechť platí (iii); pak ale $\mathbf{u}_i \in [\mathbf{u}_1, \ldots, \mathbf{u}_k] =$

$= [\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}, \mathbf{u}_{i+1}, \ldots, \mathbf{u}_k] = L(\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}, \mathbf{u}_{i+1}, \ldots, \mathbf{u}_k)$, tzn. $\mathbf{u}_i = p_1\mathbf{u}_1 + \ldots$ $\ldots + p_{i-1}\mathbf{u}_{i-1} + p_{i+1}\mathbf{u}_{i+1} + \ldots + p_k\mathbf{u}_k$, kde $p_j \in T$. Pak po úpravě dostáváme:

$$p_1 \mathbf{u}_1 + \ldots + p_{i-1} \mathbf{u}_{i-1} + (-1)\mathbf{u}_i + p_{i+1} \mathbf{u}_{i+1} + \ldots + p_k \mathbf{u}_k = \mathbf{o}$$

odkud již plyne, že vektory $\mathbf{u}_1, \ldots, \mathbf{u}_k$ jsou lineárně závislé.]

Poznámka: je třeba si uvědomit, že část (ii) předchozí věty nám zajišťuje pouze existenci vektoru, který lze vyjádřit jako lineární kombinaci zbývajících vektorů. Nelze tedy obecně tvrdit, že každý z lineárně závislých vektorů $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ se dá vyjádřit jako lineární kombinace zbývajících vektorů. Např. ve vektorovém prostoru $\mathbf{R}^2$ jsou vektory:

$$\mathbf{u}_1 = (0,1), \qquad \mathbf{u}_2 = (1,1), \qquad \mathbf{u}_3 = (0,-2)$$

lineárně závislé (neboť $2.\mathbf{u}_1 + 0.\mathbf{u}_2 + 1.\mathbf{u}_3 = \mathbf{o}$), ale přitom je zřejmé, že vektor $\mathbf{u}_2$ nelze vyjádřit jako lineární kombinaci vektorů $\mathbf{u}_1, \mathbf{u}_3$.

Důsledek. *Nechť V je vektorový prostor nad T a nechť (3) je konečná posloupnost vektorů z V. Pak platí:*

1. *obsahuje-li posloupnost (3) nulový vektor, pak je lineárně závislá*
2. *obsahuje-li posloupnost (3) dva stejné vektory, pak je lineárně závislá*
3. *je-li nějaká posloupnost vybraná ze (3) lineárně závislá, pak je i (3) lineárně závislá*
4. *je-li (3) lineárně nezávislá, pak každá posloupnost vybraná ze (3) je lineárně nezávislá.*

[D ů k a z: všechna tvrzení důsledku plynou přímo z definice lineární závislosti, resp. z předchozí věty.]

Na závěr paragrafu uvedeme nyní větu, která patří k nejdůležitějším větám celé teorie vektorových prostorů.

Věta 3.3. (Steinitzova věta o výměně). *Nechť V je vektorový prostor nad T; $\mathbf{u}_1, \ldots, \mathbf{u}_r, \mathbf{v}_1, \ldots, \mathbf{v}_s \in V$. Nechť vektory $\mathbf{u}_1, \ldots, \mathbf{u}_r$ jsou lineárně nezávislé a nechť $\mathbf{u}_i \in L(\mathbf{v}_1, \ldots, \mathbf{v}_s)$, pro $i = 1, \ldots, r$. Potom platí:*

1. *$r \leqslant s$*
2. *při vhodném přečíslování vektorů $\mathbf{v}_1, \ldots, \mathbf{v}_s$ je*

$$L(\mathbf{v}_1, \ldots, \mathbf{v}_s) = L(\mathbf{u}_1, \ldots, \mathbf{u}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_s)$$

[D ů k a z: provedeme matematickou indukcí vzhledem k r.

α) nechť $r = 1$; pak je jistě $r \leqslant s$. Z předpokladů věty dále plyne, že $\mathbf{u}_1 \neq \mathbf{o}$

(podle (5)) a je $\mathbf{u}_1 = t_1\mathbf{v}_1 + \ldots + t_s\mathbf{v}_s$. Pak ale alespoň jedno z čísel $t_1, \ldots, t_s$ musí být nenulové. Přečíslujme vektory $\mathbf{v}_1, \ldots, \mathbf{v}_s$ tak, aby $t_1 \neq 0$. Potom:

$$\mathbf{v}_1 = \frac{1}{t_1}\mathbf{u}_1 - \frac{t_2}{t_1}\mathbf{v}_2 - \ldots - \frac{t_s}{t_1}\mathbf{v}_s$$

tzn. $\mathbf{v}_1 \in L(\mathbf{u}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$. Triviálně je $\mathbf{v}_2, \ldots, \mathbf{v}_s \in L(\mathbf{u}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$, a tedy podle důsledku V.3.1. je $L(\mathbf{v}_1, \ldots, \mathbf{v}_s) \subseteq L(\mathbf{u}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$. Opačnou inklusi dostaneme stejným způsobem (užitím předpokladu $\mathbf{u}_1 \in L(\mathbf{v}_1, \ldots, \mathbf{v}_s)$), a tedy platí žádaná rovnost $L(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s) = L(\mathbf{u}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s)$.

β) předpokládáme, že tvrzení věty platí pro $1, 2, \ldots, r-1$ $(r \geqslant 2)$ a dokážeme je pro r.

Podle předpokladu a předchozího důsledku jsou vektory $\mathbf{u}_1, \ldots, \mathbf{u}_{r-1}$ lineárně nezávislé, tzn. (podle indukčního předpokladu) $r - 1 \leqslant s$ a po vhodném přečíslování je:

(6) $\quad L(\mathbf{v}_1, \ldots, \mathbf{v}_s) = L(\mathbf{u}_1, \ldots, \mathbf{u}_{r-1}, \mathbf{v}_r, \ldots, \mathbf{v}_s)$

Ale podle předpokladu věty je $\mathbf{u}_r \in L(\mathbf{v}_1, \ldots, \mathbf{v}_s) = L(\mathbf{u}_1, \ldots, \mathbf{u}_{r-1}, \mathbf{v}_r, \ldots, \mathbf{v}_s)$, odkud především plyne, že $r - 1 < s$ (jinak spor s lineární nezávislostí vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_r$), tzn. platí $r \leqslant s$.

Dále lze psát

(7) $\quad \mathbf{u}_r = t_1\mathbf{u}_1 + \ldots + t_{r-1}\mathbf{u}_{r-1} + t_r\mathbf{v}_r + \ldots + t_s\mathbf{v}_s$

přičemž alespoň jedno z čísel $t_r, \ldots, t_s$ musí být nenulové (jinak opět spor s lineární nezávislostí vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_r$). Přečíslujme je tak, aby $t_r \neq 0$. Potom:

(8) $$\mathbf{v}_r = -\frac{t_1}{t_r}\mathbf{u}_1 - \ldots - \frac{t_{r-1}}{t_r}\mathbf{u}_{r-1} + \frac{1}{t_r}\mathbf{u}_r - \frac{t_{r+1}}{t_r}\mathbf{v}_{r+1} - \ldots - \frac{t_s}{t_r}\mathbf{v}_s$$

Podle důsledku V.3.1. (užitím (7) a (8)) dostáváme, že $L(\mathbf{u}_1, \ldots, \mathbf{u}_{r-1}, \mathbf{v}_r, \ldots, \mathbf{v}_s) = L(\mathbf{u}_1, \ldots, \mathbf{u}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_s)$. Odsud a z (6) pak plyne, že $L(\mathbf{v}_1, \ldots, \mathbf{v}_s) = L(\mathbf{u}_1, \ldots, \mathbf{u}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_s)$, což je žádaná rovnost.]

§4. Báze a dimenze vektorového prostoru

Definice: Nechť V je vektorový prostor nad T. Konečná posloupnost vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_n$ z V se nazývá **báze vektorového prostoru** V, jestliže platí:

(i) vektory $\mathbf{u}_1, \ldots, \mathbf{u}_n$ jsou lineárně nezávislé

(ii) vektory $\mathbf{u}_1, \ldots, \mathbf{u}_n$ generují vektorový prostor V, tzn. $[\mathbf{u}_1, \ldots, \mathbf{u}_n] = V$.

Poznámka: místo obratu "konečná posloupnost vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_n$ je bází V" budeme častěji říkat stručně "vektory $\mathbf{u}_1, \ldots, \mathbf{u}_n$ jsou bází V".

Dále si uvědomme, že předchozí definice nezaručuje existenci báze ani nic neříká o počtu bází ve V. Celou situaci si nejprve ilustrujme na několika příkladech.

Příklad 4.1.: Z příkladů 3.1. a 3.2. bezprostředně plyne, že:

1. vektory (1,0), (0,1) jsou bází vektorového prostoru $\mathbf{R}^2$; podobně vektory (1,1), (1,2) jsou též bází $\mathbf{R}^2$. Zřejmě vektorový prostor $\mathbf{R}^2$ má nekonečně mnoho různých bází. Na druhé straně, např. vektory (0,2), (1,1), (0,1), resp. (1,3), (2,1), (1,−1), (−2,3), resp. (1,2), (2,4), resp. (1,2) nejsou bází $\mathbf{R}^2$.

2. Vektory $\mathbf{e}_1 = (1,0, \ldots, 0), \ldots, \mathbf{e}_n = (0, \ldots, 0,1)$ jsou bází vektorového prostoru T^n.

3. Vektory (polynomy) $\mathbf{f}_1 = 1, \mathbf{f}_2 = x, \ldots, \mathbf{f}_{n+1} = x^n$ jsou bází vektorového prostoru $\mathbf{R}_n[x]$.

Příklad 4.2.:

1. Nulový vektorový prostor $V = \{\mathbf{o}\}$ nemá bázi (neboť libovolná konečná posloupnost vektorů z V má tvar $\mathbf{o}, \mathbf{o}, \ldots, \mathbf{o}$, a je tedy lineárně závislá).

2. Vektorový prostor $\mathbf{R}[x]$ nemá bázi (neboť žádná konečná posloupnost vektorů (polynomů) z $\mathbf{R}[x]$ negeneruje celý prostor $\mathbf{R}[x]$. Je-li totiž $\mathbf{g}_1, \ldots, \mathbf{g}_n$ libovolná konečná posloupnost polynomů z $\mathbf{R}[x]$ a jestliže polynom $\mathbf{g}_i$ má stupeň k_i, potom jistě existuje přirozené číslo t s vlastností: $t > k_i$ pro každé $i = 1, \ldots, n$. Pak ale např. polynom $\mathbf{g} = x^t$ se nedá napsat jako lineární kombinace polynomů $\mathbf{g}_1, \ldots, \mathbf{g}_n$ a je tedy $[\mathbf{g}_1, \ldots, \mathbf{g}_n] \subsetneq \mathbf{R}[x]$.).

Rozebereme-li si předchozí definici podrobněji, pak vidíme, že báze $\mathbf{u}_1, \ldots, \mathbf{u}_n$ vektorového prostoru V je z hlediska generátorů "nejchudobnější" posloupností vektorů. Přesněji řečeno, pokud bychom některý z vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_n$ vypustili, pak zbývající vektory už nebudou generovat vektorový prostor V (plyne z V.3.2. - rozmyslete si podrobně jak). Na druhé straně, z hlediska lineární nezávislosti je báze "nejbohatší" posloupností vektorů z V, jak v dalším ukážeme.

Definice: Řekneme, že konečná posloupnost vektorů $\mathbf{u}_1, \ldots, \mathbf{u}_n$ z V je **maximální lineárně nezávislá posloupnost vektorů** ve V, jestliže