MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA

BAKALÁŘSKÁ PRÁCE

Základy matematiky, sbírka příkladů

Brno 2007

Michal Hejsek

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně s použitím uvedené literatury.

V Brně dne 14. května 2007 ....

Děkuji touto cestou RNDr. Pavlu Horákovi za cenné rady a připomínky, které mi poskytl při zpracování bakalářské práce.

OBSAH

Úvod **5**

Kapitola 1: Opakování a doplnění středoškolské látky **7**
§2: Základní množinové pojmy 7
§3: Základní vlastnosti celých čísel 10
§4: Relace 12
§5: Zobrazení 16
§6: Uspořádané množiny 20
§7: Ekvivalence a rozklady 23

Kapitola 2: Základní algebraické struktury **25**
§1: Struktury s jednou operací 25
§2: Podstruktury struktur s jednou operací 28
§3: Struktury se dvěma operacemi a jejich podstruktury 32
§4: Číselná tělesa 33

Seznam použité literatury **35**

ÚVOD

Cílem mé bakalářské práce bylo vytvořit sbírku řešených příkladů k předmětu M1125 Základy matematiky, který je povinným předmětem v bakalářském studijním programu Matematika, studijních oborech Matematika se zaměřením na vzdělávání a Matematika pro víceoborové studimu na Přírodovědecké fakultě Marsarykovy Univerzity. Ve své práci se přitom zaměřuji zejména na příklady testového charakteru, tj. na příklady ve kterých k řešení nedojdeme na základě výpočtu, ale na základě znalosti a pochopení definic a tvrzení základních matematických pojmů. Řešení příkladů doplňuji komentáři v návaznosti na probíranou látku.

Příklady jsou vybrány ze skript: Pavel Horák, Cvičení z algebry a teoretické aritmetiky I. Jedná se o příklady, které jsou ve skriptech označeny kromě čísla ještě písmenem A. Na rozdíl od těchto skript používám v příkladech místo označení $\mathbb{K}$ množiny všech komplexních čísel symbol $\mathbb{C}$. V příkladu 1.5.A5 jsme spolu s RNDr. Pavlem Horákem pozměnili zadání příkladu. Větu "co všechno lze říci o počtu prvků konečné k-prvkové množiny A", jsme nahradili větou "co všechno lze říci o počtu prvků konečné neprázdné k-prvkové množiny A". Jsou vynechány příklady z podkapitoly základní logické pojmy a příklady 2.3.A5 až A9 a příklad 2.4.A9, protože skripta odpovídají předmětu Algebra a teoretická aritmetika I. z roku 1991, zatímco nyní se používají k předmětu Základy matematiky a Lineární algebra a geometrie 1, ve kterých jsou drobné odchylky. Zkratka "U.p." zde znamená "Udejte příklad".

Práce je rozdělena do dvou kapitol. V první kapitole se zabývám příklady, které opakují a doplňují středoškolskou látku. Kapitola se dělí na šest částí a to na základní množinové pojmy, základní vlastnosti celých čísel, relace, zobrazení, uspořádané množiny a ekvivalence a rozklady. Druhá kapitola se zabývá základními algebraickými strukturami, kterými jsou struktury s jednou operací, podstruktury struktur s jednou operací, struktury se dvěma operacemi a jejich podstruktury a číselná tělesa.

Odkazy na věty, které v práci uvádím, se týkají vět a definic ze skript Pavel Horák, Základy matematiky, 2006.

V textu je používána běžná symbolika známá ze střední školy nebo taková, která je definována ve skriptech Pavel Horák, Základy matematiky. Nově zaváděná označení, která nejsou uvedena v těchto skriptech, jsou v práci vždy řádně definována před příklady, ve kterých se používají.

Pro označování základních číselných množin jsou v textu použity následující symboly:

$\mathbb{N}$ ... množina všech přirozených čísel
$\mathbb{Z}$ ... množina všech celých čísel
$\mathbb{Q}$ ... množina všech racionálních čísel
$\mathbb{R}$ ... množina všech reálných čísel
$\mathbb{C}$ ... množina všech komplexních čísel.

Tato práce je určena především jako učební text pro studenty matematiky, kteří mají zapsaný předmět M1125 a M1120. Studenti tento text mohou nalézt v Informačním systému pod odkazem Závěrečná práce v mém profilu. Samotná práce je vysázena systémem LaTeX.

Nyní bych se rád zamyslel nad tím, jak jsem přistupoval k řešení těchto příkladů v prvním semestru mého studia a nyní, když jsem tyto příklady řešil znovu. Již v prvním semestru jsem si všiml, že existují rozdíly ve znalostech jednotlivých studentů. Někteří si dokázali poradit při řešení příkladů snadno, někteří hůře a někteří vůbec. Podle mě je to dáno tím, z jaké školy a s jakými znalostmi jenotliví studenti přicházejí studovat matematiku. Jednoznačnou výhodu mají nesporně studenti gymnázií, kde se matematice věnuje mnohem více času. Jelikož já jsem studoval Obchodní akademii, kde dokonce ve čtvrtém roce studia byla matematika pouze volitelná s celkovou dotací dvě hodiny týdně, musím přiznat, že moje znalosti byly velmi chatrné a že při řešení příkladů uvedených v této bakalářské práci jsem prožíval v prvním semestru svého studia leckdy pořádná muka a k řešení jsem se nedostával snadnou cestou, spíše bych řekl, že to hodně bolelo. Ze cvičení jsem se vracel domů deprimovaný, naštěstí jsem nepodlehl skepsi a pečlivým a hlavně pravidelným studiem jsem postupně zaceloval svoje mezery ve svých matematických znalostech. To považuji za hlavní příčinu toho, že jsem se vůbec dostal až k bakalářským státnicím a k vypracování této práce vůbec.

Co mi dělalo největší problémy při řešení těchto příkladů v prvním semestru? Z dnešního pohledu si myslím, že to bylo hlavně to, že jsem toho o matematice nevěděl příliš mnoho, dnes mi dokonce připadá, že skoro vůbec nic. Neznal jsem základní postupy při řešení příkladů, neměl jsem rozvinuté matematické myšlení. Dokonce mi připadalo divné, až nesmyslné zdůvodňovat řešení (např. když příklad nemá řešení, tak uvést proč). Musím se přiznat, že jsem sám přišel na řešení nějaké příkladu jen velmi zřídka a ani to možná nebylo možné při "rychlém" výkladu přednášek a "spěchu" při cvičeních. Některým řešením jsem nerozuměl ani před zkouškou.

Vzhledem k tomu, že mi řešení příkladů v prvním semestru moc nešlo, měl jsem trochu obavy, zda vůbec budu schopný vypracovat kvalitní bakalářskou práci. Samotné řešení příkladů však šlo překvapivě docela snadno. Přičítám to hlavně získaným zkušenostem a znalostmi v dosavadním průběhu studia. Největší problém už od prvního semestru je určení nutné, ale ne dostatečné podmínky a to mi zůstalo dodnes. K těmto typům příkladům mám asi nějaký blok, ale musím přiznat, že právě tyto příklady dokonale prověří znalosti studenta. Co se však ukázalo jako největší problém při vypracování mojí bakalářské práce, bylo vhodné okomentování řešení. Nad tím jsem strávil nejvíce času a také jsem v něm dělal nejvíce oprav. Abych udělal skutečně kvalitní okomentování musel jsem se pořádnět zamyslet a samozřejmě si také pořádně osvěžit definice a věty k dané látce.

Dnes mohu odpovědně říci, že pečlivé studium i ostatních předmětů mi pomohl a pomáhá k řešení složitějších příkladů a určitě se vyplatí.

KAPITOLA 1:

OPAKOVÁNÍ A DOPLNĚNÍ STŘEDOŠKOLSKÉ LÁTKY

§2: ZÁKLADNÍ MNOŽINOVÉ POJMY

[**1.2.A1**]. U.p. konečné množiny M, jejímiž prvky jsou nekonečné množiny.

Řešení: $M = \{\mathbb{N}, \mathbb{Z}\}$

Komentář: Nejdříve vybereme konečný počet nekonečných množin (třeba jednu nebo dvě). Ty pak použijeme jako prvky výsledné množiny M.

[**1.2.A2**]. U.p. nekonečné množiny M, jejímiž prvky jsou konečné množiny.

Řešení: $M = \{\{1\}, \{2\} \ldots\}$

Komentář: Zvolíme si nějakou "jednoduchou" nekonečnou množinu, např. $\mathbb{N}$. Z každého prvku vytvoříme jednoprvkovou množinu.

[**1.2.A3**]. U.p. množin A, B tak, aby množina $A \times 2^B$ měla 18 prvků.

Řešení: $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}, B = \{1\}$

Komentář: Množiny A, B zřejmě musí být konečné. Pak množina 2^B má počet prvků rovnu mocnině čísla 2. Počet prvků kartézského součinu dvou konečných množin je roven součinu počtu jejích prvků. Číslo 18 lze vytvořit z těchto součinů: $1.18, 2.9, 3.6.$V těchto součinech jsou dvě mocniny dvojky 1 a 2. Množina 2^B musí mít tedy 2 prvky a množina A musí mít 9 prvků. Množina B je tedy prázdná nebo jednoprvková a úloha má 2 možná řešení.

[**1.2.A4**]. U.p. množin A, B, C takových, že $A \cap B \subseteq A \cap C$ a $B \nsubseteq C$.

Řešení: $A = \emptyset, B = \{1\}, C = \{2\}$

Komentář: Prázdná množina je podmnožinou každé množiny. Zvolíme-li množinu A jako prázdnou, pak $A \cap B = \emptyset$ a stačí vzít jakékoliv množiny B a C takové, že $B \nsubseteq C$.

[**1.2.A5**]. U.p. nekonečné množiny A a konečné množiny B tak, že $A - B = \emptyset$.

Řešení: Neexistuje.
Zřejmě $A - B = \emptyset \Leftrightarrow A \subseteq B$. Ale nekonečná množina nemůže být podmnožina konečné množiny.

[**1.2.A6**]. U.p. dvou různých množin A, B tak, že $A - B \subseteq B - A$.

Řešení: $A = \emptyset, B = \{1\}$

Komentář: Množina A musí být podmnožinou množiny B.

[**1.2.A7**]. U.p. množiny A, která má právě 3 podmnožiny.

Řešení: Neexistuje.
Množina všech podmnožin konečné množiny má vždy počet prvků rovnu číslu, které je mocninou dvojky.

[**1.2.A8**]. U.p. množin A, B tak, aby množina $A \times B$ měla právě 32 podmnožin.

Řešení: Například $A = \{1, 2, 3, 4, 5\}, B = \{1\}$
Komentář: Množina $A \times B$ musí mít 5 prvků. Zvolme například množinu A 5-ti prvkovou a množinu B jedno prvkovou. Jsou možná pouze 2 řešení.

[**1.2.A9**]. Nechť $A = \{0, 1, 2\}$. Přečtěte nahlas následující výroky a rozhodněte, které z nich jsou pravdivé a které nepravdivé:

a) $0 \in A$ b) $\{0\} \in A$ c) $0 \subseteq A$ d) $\{0\} \subseteq A$ e) $\emptyset \in A$ f) $\emptyset \subseteq A$

g) $\{\emptyset\} \in A$ h) $\{\emptyset\} \subseteq A$ i) $\{2\} \in \{2, \{2\}\}$ j) $\{2\} \subseteq \{2, \{2\}\}$.

Řešení:

a) Nula je prvkem A. Pravdivý výrok.

b) Množina sestávající se z prvku nula je prvkem A. Nepravdivý výrok.

c) Nula je podmnožinou A. Nepravdivý výrok.

d) Množina sestávající se z prvku nula je podmnožinou A. Pravdivý výrok

e) Prázdná množina je prvkem A. Nepravdivý výrok.

f) Prázdná množina je podmnožinou A. Pravdivý výrok.

g) Množina sestávající se z prázdné množiny je prvkem A. Nepravdivý výrok.

h) Množina sestávající se z prázdné množiny je podmnožinou A. Nepravdivý výrok.

i) Množina sestávající se z prvku 2 je prvkem množiny sestávající se z 2 a množiny sestávající se z 2. Pravdivý výrok.

j) Množina sestávající se z prvku 2 je podmnožinou množiny sestávající se z 2 a množiny sestávající se z 2. Pravdivý výrok.

Komentář:

a) - h) Množina A má 3 prvky: 0,1,2. Zároveň množina A má 8 podmnožin: $\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}$. Při řešení stačí pouze zkontrolovat, zda se daný objekt nachází mezi prvky A, resp. mezi podmnožinami A.

i) - j) Jedná se o situaci, kdy daný objekt je zároveň prvkem množiny a také je podmnožinou množiny.

[**1.2.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

c) je nutná a dostatečná

pro to, aby množiny A, B byly různé.

Řešení:

a) $A \not\subseteq B$

b) $A = \{1\}, B = \{2\}$

c) $A \not\subseteq B \vee B \not\subseteq A$

Komentář:

b) U příkladů tohoto typu je vhodné uvést jeden konkrétní případ.

§3: ZÁKLADNÍ VLASTNOSTI CELÝCH ČÍSEL

[**1.3.A1**]. U.p. celých čísel a, b, c tak, že $a \mid b \cdot c$, ale $a \nmid b \wedge a \nmid c$.

Řešení: Řešení je nekonečně mnoho, například $a = 6, b = 3, c = 2$.

Komentář: Zvolme číslo a jako součin dvou prvočísel b, c.

[**1.3.A2**]. U.p. celých čísel x, y tak, že $7 \nmid (21x - 56y)$.

Řešení: Neexistuje.
Jestliže číslo dělí jiná dvě čísla, pak dělí i jejich libovolnou lineární kombinaci. Zde $7 \mid 21 \wedge 7 \mid 56$, tj. 7 musí dělit i $(21x - 56y)$.

[**1.3.A3**]. U.p. dvou různých celých čísel a, b tak, že $a \mid b \wedge b \mid a$.

Řešení: Nekonečně mnoho řešení, například $a = 7, b = -7$.

Komentář: Nelze se omezovat pouze na kladná nebo záporná čísla. Jedná se vždy o nenulová čísla lišící se znaménkem.

[**1.3.A4**]. U.p. celého čísla a, které po dělení 8 dává zbytek -2.

Řešení: Neexistuje.
Podle věty o dělení se zbytkem celých čísel je zbytek vždy nezáporné číslo.

Pro potřeby následujících 2 příkladů zavedeme symbol (a, b), který značí nezáporný největší společný dělitel celých čísel a, b. Tento symbol není v učebním textu zaváděn.

[**1.3.A5**]. U.p. celých čísel a, b, k nimž neexistuje (a, b).

Řešení: Neexistuje.
Podle Bezoutovy věty (viz. věta 4.3.3) existuje pro každá dvě celá čísla jejich největší společný dělitel, přičemž, je-li d jejich největší společný dělitel, pak $\{d, -d\}$ je množinou všech jejich největších společných dělitelů, tzn. existuje i záporný největší společný dělitel dvou celých čísel.

[**1.3.A6**]. U.p. dvou různých celých čísel a, b tak, že $(a, b) = -a$.

Řešení: $a = -3, b = 6$

Komentář: Podle věty 4.3.2. nalezneme k číslu a takové číslo b, pro které platí $(a, b) = a$.

[**1.3.A7**]. U.p. celých čísel a, b tak, že $a \equiv b \pmod 9 \wedge b \not\equiv a \pmod 9$.

Řešení: Neexistuje.
Jestliže platí, že $a \equiv b \pmod m$, pak podle věty 4.8.2. je také $b \equiv a \pmod m$.

[**1.3.A8**]. Uveďte, kolik existuje záporných čísel, která jsou kongruentní s číslem 6 podle modulu 7.

Řešení: Nekonečně mnoho řešení.

Komentář: Řešením jsou všechna záporná čísla ze zbytkové třídy C_6 (podle modulu 7), tj. $\{\ldots, -15, -8, -1\}$, [**1.3.A9**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby celá čísla a, b byla kongruentní podle modulu 6.

Řešení:

a) $a \equiv b \pmod{3}$

b) $a = 7, b = 1$

[**1.3.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby celá čísla a, b nebyla nesoudělná.

Řešení:

a) a, b nejsou různá prvočísla.

b) $a = 6, b = 9$

§4: RELACE

[**1.4.A1**]. Nechť $M = \{x, y, z\}$. Uveďte, kolik lze definovat různých relací

a) mezi množinami M a 2^M

b) mezi množinami M a $\emptyset$

c) na množině M

d) na množině $M \times M$.

Řešení:

a) 2^{24}

b) 1

c) 2^9

d) 2^{81}

Komentář:

a) Podle definice je relace mezi množinami A, B libovolná podmnožina kartézského součinu těchto množin. Kartézský součin množin M a 2^M má 24 prvků. Počet podmnožin tohoto kartézského součinu má právě 2^{24} prvků (relací).

b) Kartézský součin libovolné neprázdné množiny s prázdnou množinou je prázdná množina, která má právě jednu podmnožinu a to sebe samu.

c) Relace na libovolné neprázdné množině A je libovolná podmnožina kartézského součinu $A \times A$. Kartézský součin $A \times A$ má 9 prvků, podmnožin tohoto kartézského součinu je 2^9.

d) Postupujeme podle definice relace na libovolné neprázdné množině A. Místo množiny A ale uvažujeme množinu $M \times M$. Kartézský součin $(M \times M) \times (M \times M)$ má 81 prvků, podmnožin tohoto kartézského součinu je 2^{81}.

[**1.4.A2**]. U.p. neprázdné relace ϱ mezi množinami $\mathbb{N}$ a $\mathbb{Z}$ a neprázdné relace σ mezi množinami $\mathbb{Z}$ a $\mathbb{Q}$ tak, že složená relace $\sigma \circ \varrho$ je prázdnou relací.

Řešení: $\varrho = \{(1, -2), (5, 0)\}, \sigma = \{(10, \frac{1}{2})\}$

Komentář: Nechť $a \in \mathbb{N}, c \in \mathbb{Q}$. Aby složením relací ϱ a σ byla prázdná množina, nesmí existovat $b \in \mathbb{Z}$ tak, že $(a, b) \in \varrho \wedge (b, c) \in \sigma$. Řešení je nekonečně mnoho.

[**1.4.A3**]. U.p. relací ϱ, σ na množině $M = \{a, b\}$ tak, že ϱ, σ nejsou univerzálními relacemi, ale $\sigma \circ \varrho$ je univerzální relací na M.

Řešení: $\varrho = \{(a, a), (b, a), (b, b)\}, \sigma = \{(a, a), (a, b), (b, b)\}$

Komentář: Nejprve si uvědomme, že univerzální relace na libovolné množině A je množina $A \times A$ samotná, neboli každý prvek z množiny A je v relaci s každým prvkem z množiny A. Pro větší názornost si zobrazme tento příklad graficky. První, druhý i třetí sloupec budou tvořit prvky z množiny A (prvky kreslíme pod sebe). Pokud jsou dva prvky v relaci, spojíme je orientovanou šipkou. Při relaci $\sigma \circ \varrho$ vede orientovaná šipka z bodu prvního sloupce do bodu třetího sloupce právě když tuto šipku lze ”složit” ze šipky patřící do grafu relace ϱ, začínající v prvku z prvního sloupce a šipky patřící do grafu relace σ končící v prvku třetího sloupce, přičemž obě šipky mají společný bod ve druhém sloupci. Vybereme 2 vhodné neuniverzální relace, aby jejich složením byla relace univerzální. Jedno z možných řešení je na obrázku.

$$\begin{tikzcd}
a \arrow[r, "\varrho"] & a \arrow[r, "\sigma"] \arrow[dr] & a \\
b \arrow[r] \arrow[ur] & b \arrow[r] & b
\end{tikzcd}$$

[**1.4.A4**]. U.p. množiny M a relace ϱ na M, která je současně symetrická a antisymetrická.

Řešení: $M = \{x, y, z\}$, $\varrho = \{(x, x), (z, z)\}$

Komentář: Je vhodné použít vyjádření relace ϱ pomocí tabulky. Sestrojme tabulku, která bude vyhovovat zadání a to tak, že:

1) je symetrická podle hlavní diagonály

2) dvě různá políčka symetrická podle hlavní diagonály obsahují nejvýše jednu jedničku.

Aby daná relace ϱ byla symetrická a zároveň antisymetrická musí tedy dvě různá políčka symetrická podle hlavní diagonály obsahovat nuly. Pokud jde o hlavní diagonálu, ta nuly obsahovat může, ale nemusí.

	x	y	z
x	1	0	0
y	0	0	0
z	0	0	1

[**1.4.A5**]. U.p. množiny M a relace ϱ na M, která není symetrická a není antisymetrická.

Řešení: $M = \{x, y, z\}$, $\varrho = \{(x, y), (x, z), (y, x), (y, z), (z, y)\}$

Komentář: Uvažme tabulkovou reprezentaci relace. Aby relace ϱ nebyla symetrická a nebyla antisymetrická, musí být množina M alespoň 3-prvková. Dále, některé dvě různé políčka symetrická podle hlavní diagonály obsahují jednu jedničku a jednu nulu (pak relace není symetrická) a některé dvě políčka symetrické podle hlavní diagonály obsahují současně jedničku (není antisymetrická).

	x	y	z
x	0	1	1
y	1	0	1
z	0	1	0

[**1.4.A6**]. U.p. relace ϱ, různé od relace rovnosti, na množině $\mathbb{Z}$ tak, že ϱ je reflexivní a není úplná.

Řešení: $\varrho = \{(x,x) \,|\, x \in \mathbb{Z}\} \cup \{(1,3)\}$

Komentář: Relace ϱ, která není úplná, se z tabulky relace pozná tak, že alespoň jedna dvojice různých políček symetrických podle hlavní diagonály obsahuje nuly. K relaci rovnosti na množině $\mathbb{Z}$ tedy např. přidáme jednu uspořádanou dvojici různých čísel z množiny všech celých čísel.

[**1.4.A7**]. U.p. relace ϱ na množině $\mathbb{N}$, která je úplná a není reflexivní.

Řešení: Neexistuje.
Relace, která je úplná je současně reflexivní.

[**1.4.A8**]. U.p. množiny A tak, aby relace inkluze $\subseteq$ na množině 2^A byla úplnou relací.

Řešení: $A = \emptyset$

Komentář: Tato úloha má právě 2 řešení. A sice: množina A je prázdná nebo jednoprvková. Jinak po rozepsání do tabulky zjišťujeme, že relace $\subseteq$ na možině 2^A není úplná, protože pro $A = \{a_1, a_2, \dots\}$ neplatí, že $\{a_1\} \subseteq \{a_2\} \vee \{a_2\} \subseteq \{a_1\}$.

[**1.4.A9**]. Dokažte, že relace dělitelnosti na množině $\mathbb{N}$ je antisymetrická, kdežto relace dělitelnosti na množině $\mathbb{Z}$ není antisymetrická.

Řešení:

a) Dokážeme, že relace dělitelnosti na $\mathbb{N}$ je antisymetrická. Nechť $x, y \in \mathbb{N} \wedge x \mid y \wedge y \mid x \Rightarrow \exists\, c_1, c_2 \in \mathbb{N} : y = c_1 \cdot x \wedge x = c_2 \cdot y \Rightarrow$ po dosazení dostáváme $y = (c_1 \cdot c_2) y \Rightarrow$ po vykrácení (které je zde možné) $c_1 \cdot c_2 = 1 \Rightarrow$ (protože $c_1, c_2 \in \mathbb{N}$) $c_1 = 1 \wedge c_2 = 1 \Rightarrow x = 1 \cdot y = y$.

b) Dokážeme, že relace dělitelnosti na $\mathbb{Z}$ není antisymetrická a to tak, že uvedeme konkrétní protipříklad. Např. pro $x = 2, y = -2$ dostáváme $2 \mid -2 \wedge -2 \mid 2 \wedge 2 \neq -2$, tzn. relace dělitelnosti není antisymetrická.

[**1.4.A10**]. Popište, jak se z tabulky relace (na konečné množině) pozná, že tato relace je, resp. není

a) reflexivní

b) symetrická

c) antisymetrická

d) úplná.

Řešení:

a) je reflexivní: v hlavní diagonále jsou samé jedničky,
není reflexivní: v hlavní diagonále je alespoň jedna nula,

b) je symetrická: tabulka je symetrická podle hlavní diagonály,
není symetrická: tabulka není symetrická podle hlavní diagonály,

c) je antisymetrická: dvě různá políčka symetrická podle hlavní diagonály obsahují nejvýše jednu jedničku,
není antisymetrická: dvě různá políčka symetrická podle hlavní diagonály obsahují dvě jedničky,

d) je úplná: v hlavní diagonále jsou samé jedničky a dvě různá políčka symetrická podle hlavní diagonály obsahují alespoň jednu jedničku,
není úplná: v hlavní diagonále nejsou samé jedničky nebo alespoň dvě různá políčka symetrická podle hlavní diagonály obsahují dvě nuly.

§5: ZOBRAZENÍ

[**1.5.A1**]. U.p. zobrazení $f : \mathbb{Z} \to \mathbb{N}$, které

a) je injektivní a není surjektivní

b) je surjektivní a není injektivní.

Řešení:

a)

$$f(x) = \begin{cases} 2x+1 & x > 0 \\ -2x+2 & x \leq 0 \end{cases}$$

b)

$$f(x) = \begin{cases} |x| & x \neq 0 \\ 1 & x = 0 \end{cases}$$

Komentář:

a) Kladná celá čísla zobrazujeme postupně na lichá přirozená čísla počínaje trojkou. Nekladná celá čísla zobrazujeme postupně na sudá přirozená čísla. Takové zobrazení je injektivní, ale není surjektivní, protože $1 \in \mathbb{N}$ nemá žádný vzor při zobrazení f.

b) Zobrazení f je surjektivní, ale není injektivní, protože dvě různá čísla 1 a -1 se obě zobrazí na 1. Zkuste si nakreslit sami část obrázku.

[**1.5.A2**]. U.p. injektivního zobrazení $f : A \times A \to 2^A$, je-li:

a) $A = \{a, b\}$

b) $A = \{a, b, c\}$.

Řešení:

a) $f((a,a)) = \emptyset, f((a,b)) = \{a\}, f((b,a)) = \{b\}, f((b,b)) = \{a,b\}$

b) Neexistuje.
Požadované injektivní zobrazení nelze sestrojit, protože každý prvek z množiny 2^A musí mít při zobrazení f nejvýše jeden vzor. Počet prvků $2^A = 8$ a počet prvků $A \times A = 9$. Podle definice injektiního zobrazení můžeme zobrazit 8 prvků po jednom každý na různý obraz, ale devátý již musíme zobrazit na některý prvek, který má již vzor.

Komentář:

a) Nejprve si uvědomme, jak vypadají množiny $A \times A, 2^A$. Aby zobrazení f dvou konečných množin bylo injektivní, musí být počet prvků definičního oboru menší nebo roven počtu prvků oboru hodnot a každé dva prvky z definičního oboru musí mít dva různé obrazy při zobrazení f. Počet všech různých injektiních zobrazení je roven číslu 4!.

[**1.5.A3**]. U.p. injektivního zobrazení

a) $f : \mathbb{Z} \to 2^{\mathbb{N}}$

b) $f : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$.

Řešení:

a)

$$f(x) = \begin{cases} \{-x\} & x < 0 \\ \emptyset & x = 0 \\ \{x, x+1\} & x > 0 \end{cases}$$

b) $f : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$
$f(n) = g_n$, kde $g_n : \mathbb{N} \to \mathbb{N}$, je zobrazení definované takto:
$g_n(x) = n$, $\forall x \in \mathbb{N}$.

[**1.5.A4**]. U.p. surjektivního zobrazení

a) $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$

b) $f : 2^{\mathbb{N}} \to \mathbb{N}$

Řešení:

a)

$$f((x,y)) = \begin{cases} -\frac{x}{2} & x \text{ sudé, } y \text{ libovolné} \\ \frac{1-x}{2} & x \text{ liché, } y \text{ libovolné} \end{cases}$$

b)

$$f(X) = \begin{cases} x & X = \{x\} \\ 1 & \text{jinak} \end{cases}$$

[**1.5.A5**]. Uveďte, co všechno lze říci o počtu prvků konečné, neprázdné k-prvkové množiny A, víte-li, že
a) existuje injektivní zobrazení $2^A \to A \times A$
b) neexistuje žádné surjektivní zobrazení $A \times A \to A^A$.

Řešení:

a) $k = 2, 3, 4$

b) $k \geq 3$

Komentář:

a) Jestliže existuje injektivní zobrazení konečné množiny A do konečné množiny B, pak počet prvků A musí být menší nebo roven počtu prvků množiny B. V našem případě je:
pro $k = 1$ je počet prvků množiny 2^A větší než počet prvků množiny $A \times A$,
pro $k = 2, 3, 4$ je počet prvků množiny 2^A menší nebo roven počtu prvků množiny $A \times A$,
pro $k > 4$ je počet prvků množiny 2^A větší než počet prvků množiny $A \times A$.

b) Jestliže neexistuje surjektivní zobrazení konečné množiny A do konečné množiny B, pak počet prvků A musí být menší než počet prvků množiny B. V našem případě je: pro $k = 1, 2$ jsou splněny podmínky pro vytvoření surjektivního zobrazení, pro $k \geq 3$ nejsou splněny podmínky pro vytvoření surjektivního zobrazení.

[**1.5.A6**]. U.p. množiny B, její vlastní podmnožiny A (t.j. $A \subset B$) a bijektivního zobrazení $f : A \to B$.

Řešení: $A = \mathbb{N}, B = \mathbb{Z}, f(x) = \begin{cases} \frac{1-x}{2} & x \text{ liché} \\ \frac{x}{2} & x \text{ sudé} \end{cases}$

Komentář: Jestliže existuje bijektivní zobrazení $f : A \to B$, pak A a B mají stejnou mohutnost. V případě konečných množin to znamená, že A a B mají stejný počet prvků. V našem případě tedy musí být množiny A, B nekonečné.

[**1.5.A7**]. U.p. zobrazení $f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}\times\mathbb{N}$, $g : \mathbb{N}\times\mathbb{N} \to \mathbb{N}\times\mathbb{N}$ takových, že $f\circ g \neq g\circ f$.

Řešení:
$f((x, y)) = (x + 1, y)$, pro $\forall\, x, y \in \mathbb{N} \times \mathbb{N}$
$g((x, y)) = (x^2, y)$, pro $\forall\, x, y \in \mathbb{N} \times \mathbb{N}$.

Komentář: Zobrazení $f \circ g$ se nerovná zobrazení $g \circ f$, protože například pro uspořádanou dvojici $(1, 2)$ je: $f \circ g(1, 2) = (2, 2)$ a $g \circ f(1, 2) = (4, 2)$, přičemž $(2, 2) \neq (4, 2)$.

[**1.5.A8**]. Nechť je $A = \{a, b\}$; u.p. zobrazení $f : 2^A \to A^A$ tak, že k tomuto zobrazení neexistuje inverzní zobrazení.

Řešení: $f(X) = id_A$ pro $\forall\, X \in 2^A$

Komentář: Aby neexistovalo inverzní zobrazení k zobrazení f, nesmí být f bijektivní. V našem případě jsme vybrali zobrazení f, které každému prvku z 2^A přiřazuje vždy identické zobrazení id_A.

[**1.5.A9**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby zobrazení $f : A \to B$ nebylo surjektivní.

Řešení:

a) B není jednoprvková

b) $A = \{1\}, B = \{2, 3\}, f(1) = 2$

[**1.5.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby zobrazení $f : A \to B$ bylo bijektivní.

Řešení:

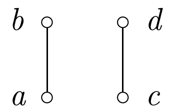
a) f je injektivní.

b) $A = B$ a $f : A \to B$ je identita.

§6: USPOŘÁDANÉ MNOŽINY

[**1.6.A1**]. Nakreslete hasseovský diagram čtyřprvkové uspořádané množiny, která má dva maximální prvky a nemá nejmenší prvek.

Řešení:



Komentář: Maximálními prvky jsou prvky b a d. Množina nemá nejmenší prvek y, tj. prvek y, pro který by platilo $y \leq x$, $\forall\, x \in M$.

[**1.6.A2**]. Nakreslete hasseovský diagram čtyřprvkové uspořádané množiny, v níž každý prvek je současně maximálním prvkem i minimálním prvkem.

Řešení:

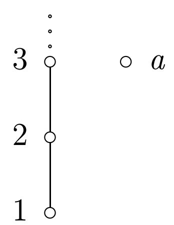
Komentář: Aby prvek x byl zároveň minimálním a maximálním, nesmí existovak prvek y takový, že $y < x \wedge x < y$, tzn. z prvku x nevede žádná čára ani nahoru ani dolu.

[**1.6.A3**]. Nakreslete hasseovský diagram konečné uspořádané množiny, která má tři minimální prvky a žádný maximální prvek.

Řešení: Neexistuje.
Konečná uspořádaná množina má vždy minimální a maximální prvek.

[**1.6.A4**]. U.p. uspořádané množiny (M, ϱ), která má jeden maximální prvek a nemá největší prvek.

Řešení: Požadovaný příklad zadáme množinovým popisem a pro větší názornost přidáme ještě část hasseovského diagramu.
$M = \mathbb{N} \cup \{a\}$, $x \,\varrho\, y \;\Leftrightarrow\; (x, y \in \mathbb{N} \wedge x \leq y) \vee (x = y = a)$
tzn. hasseovský diagram lze schématicky nakreslit takto:

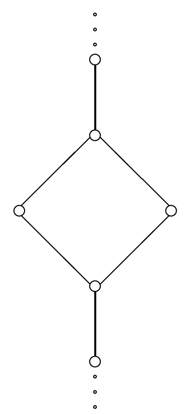


[**1.6.A5**]. U.p. uspořádané množiny (M,ϱ), která má jeden nejmenší prvek a tři minimální prvky.

Řešení: Neexistuje.
Podle věty 7.1.2. je-li některý prvek nejmenší, pak je také minimální a žádné další minimální prvky v uspořádané množině (M,ϱ) neexistují.

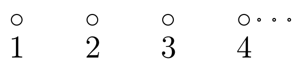
[**1.6.A6**]. U.p. uspořádané množiny (M,ϱ), která obsahuje právě dva nesrovnatelné prvky a nemá přitom žádný maximální prvek ani minimální prvek.

Řešení:



[**1.6.A7**]. U.p. nekonečné uspořádané množiny (M,ϱ), která neobsahuje žádné různé srovnatelné prvky.

Řešení: Požadovaný příklad zadáme množinovým popisem a pro větší názornost přidáme ještě část hasseovského diagramu.
$M=\mathbb{N}, x\,\varrho\,y \Leftrightarrow x=y$
tzn. hasseovský diagram lze schématicky nakreslit takto:



[**1.6.A8**]. U.p. lineárně uspořádané množiny (M,ϱ), která má dva minimální prvky.

Řešení: Neexistuje.
Řešení neexistuje, protože v lineárně uspořádané množině splývají pojmy nejmenšího a minimálního prvku viz.věta 7.3.1. Tedy v lineárně uspořádané množině existuje nejvýše jeden minimální prvek.

[**1.6.A9**]. U.p. množiny A tak, aby uspořádaná množina $(2^A,\subseteq)$ byla lineárně uspořádaná.

Řešení: $A=\{a\}$.

Komentář: Úloha má dvě možná řešení, $A = \emptyset$ nebo A je jednoprvková množina. Sestává-li se množina A alespoň ze dvou prvků, tj. $A = \{a_1, a_2, \dots\}$, pak $(2^A, \subseteq)$ není lineárně uspořádaná množina, protože např. $\{a_1\} \nsubseteq \{a_2\} \wedge \{a_2\} \nsubseteq \{a_1\}$.

[**1.6.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby v uspořádané množině (M, ϱ) neexistoval maximální prvek.

Řešení:

a) neexistuje největší prvek,

b) $(M, \varrho) = (\mathbb{N}, \leq)$.

§7: EKVIVALENCE A ROZKLADY

[1.7.A1]. U.p. relace ϱ na množině $\mathbb{Z}$, která je současně ekvivalencí i uspořádáním. Dále uveďte, kolik takových relací existuje.

Řešení: $\varrho = \{(x, x) \,|\, x \in \mathbb{Z}\}$, tzn. ϱ je relace rovnosti na $\mathbb{Z}$. Relace s požadovanými vlastnosmi je jediná.

Komentář: Aby ϱ byla současně ekvivalence a uspořádání, musí být současně reflexivní, symetrická, antisymetrická a tranzitivní. Je-li ϱ reflexivní, pak jsou v hlavní diagonále samé jedničky. Je-li ϱ symetrická, pak ve dvou různých políčkách, které jsou symetrické podle hlavní diagonály, jsou buď dvě nuly nebo dvě jedničky. Je-li ϱ antisymetrická, pak ve dvou různých políčkách symetrických podle hlavní diagonály nejsou dvě jedničky. Dohromady dostáváme, že v symetrickách políčkách podle hlavní diagonály musí být dvě nuly. Tedy ϱ musí být relací rovnosti (která je také tranzitivní).

[1.7.A2]. U.p. relace ϱ na množině $\mathbb{N}$, která je reflexivní a tranzitivní, ale není ekvivalencí ani uspořádáním.

Řešení: $\varrho = \{(x, x) \,|\, x \in \mathbb{N}\} \cup \{(1, 2), (1, 3), (2, 1)\}$

Komentář: Relace ϱ je zřejmě reflexivní a je také tranzitivní (rozmyslete si podrobně proč tomu tak je), ϱ není symetrická, protože $1 \,\varrho\, 3 \wedge 3 \,\bar{\varrho}\, 1$ a není antisymetrická, protože $1 \,\varrho\, 2 \wedge 2 \,\varrho\, 1$, tedy ϱ není ekvivalence a ϱ není uspořádání.

[1.7.A3]. U.p. relace ekvivalence ϱ na množině $\mathbb{R}$ tak, aby rozklad $\mathbb{R}/\varrho$ (tj. rozklad na $\mathbb{R}$ příslušný ekvivalenci ϱ) měl právě 3 třídy rozkladu.

Řešení: $\forall\, x, y \in \mathbb{R}$ položíme $x \,\varrho\, y \Leftrightarrow$ (x, y jsou kladná) $\vee$ ($x = y = 0$) $\vee$ (x, y jsou záporná).

Komentář: Pro řešení je nutno zadat relaci ekvivalence a myslet přitom na to, aby $\mathcal{R}/\varrho$ měl 3 třídy. V našem případě je relace zadána v řešení, přičemž následně vychází $\mathcal{R}/\varrho = \mathbb{R}^+, \mathbb{R}^-, \{0\}$.

[1.7.A4]. U.p. rozkladu na $\mathbb{R}$, který má konečně mnoho tříd, přičemž každá třída obsahuje konečně mnoho prvků.

Řešení: Neexistuje.
Protože sjednocení konečně mnoho konečných množin je konečná množina, zatímco množina $\mathbb{R}$ je nekonečná.

[1.7.A5]. U.p. rozkladu na $\mathbb{N}$, který má nekonečně mnoho tříd, přičemž každá třída obsahuje nekonečně mnoho prvků.

Řešení: $\mathcal{R} = \{\{p_i^k \,|\, k \geq 1, p_i$ prvočíslo$\} \cup \{x \,|\, x$ není mocnina jednoho provočísla$\}\}$.

Komentář: Třídy uvedeného rozkladu jsou jednak množiny sestávající se z přirozených mocnin daného prvočísla a jednak z množiny obsahující "ostatní přirozená čísla". Vzhledem k tomu, že prvočísel je nekonečně mnoho, dostáváme nekonečně mnoho tříd.

[1.7.A6]. U.p. zobrazení $f : \mathbb{R} \to \mathbb{Z}$ tak, aby rozklad příslušný zobrazení f měl nekonečně mnoho tříd rozkladu.

Řešení: $f(x) = a$ pro $x \in \langle a, a + 1)$ pro $a \in \mathbb{Z}$.

[**1.7.A7**]. U.p. zobrazení $f : \mathbb{R} \to \mathbb{Z}_3$ tak, aby rozklad příslušný zobrazení f měl

a) 2 třídy rozkladu

b) 4 třídy rozkladu.

Řešení:

a)

$$f(x) = \begin{cases} C_0 & x > 0 \\ C_1 & x \leq 0 \end{cases}$$

b) Neexistuje.
Množina $\mathbb{Z}_3$ má pouze 3 prvky.

[**1.7.A8**]. Uveďte všechny hodnoty modulu m pro které čísla -7 a 7 patří do stejné zbytkové třídy podle tohoto modulu m.

Řešení: $m = 1, 2, 7, 14$

Komentář: Čísla 7 a -7 mají po dělení modulem stejný zbytek, tzn.
$7 = k.m + r$, kde $0 \leq r < m$
$-7 = l.m + r$, kde $0 \leq r < m$
a po odečtení dostáváme $14 = (k - l).m \;\Rightarrow\; m \,|\, 14 \;\Rightarrow\; m = 1, 2, 7, 14.$

[**1.7.A9**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby relace ϱ na množině M byla ekvivalencí.

Řešení:

a) ϱ je reflexivní,

b) ϱ je relace rovnosti.

[**1.7.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby systém množin $\mathcal{M} = \{A, B\}$, kde A, $B \subseteq \mathbb{N}$, byl rozkladem na $\mathbb{N}$.

Řešení:

a) $A \neq \emptyset$

b) $A = \{2k \,|\, k \in \mathbb{N}\}$
$B = \{2k + 1 \,|\, k \in \mathbb{N}\}$

KAPITOLA 2:

ZÁKLADNÍ ALGEBRAICKÉ STRUKTURY

§1: STRUKTURY S JEDNOU OPERACÍ

[2.1.A1]. Uveďte, kolika různými způsoby je možno definovat operaci na množině $G = \{x, y, z\}$.

Řešení: $3^9 = 19\,683$ různými způsoby

Komentář: Operace na množině G je definována jako libovolné zobrazení $G \times G \to G$. Operací na množině G je tedy tolik, kolik je zobrazení $G \times G \to G$. Je-li tedy G tříprvková, pak různých zobrazení $G \times G \to G$ je právě $3^{3\times 3} = 3^9$.

[2.1.A2]. U.p. grupoidu $(G, \cdot)$ tak, že tento grupoid má jedničku, ale není pologrupou.

Řešení: $G = \{a, b, c, d\}$, operaci $\cdot$ definijeme 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

[2.1.A3]. U.p. grupoidu $(G, \cdot)$ tak, že v tomto grupoidu neplatí zákony o dělení.

Řešení: $(G, \cdot) = (\mathbb{N}, +)$

Komentář: $(\mathbb{N}, +)$ je zřejmě grupoidem. Pro $a = 7, b = 1$ jistě nenajdeme žádné $x \in \mathbb{N}$, pro které by platilo $a + x = b$, tedy v $(\mathbb{N}, +)$ neplatí zákony o dělení.

[2.1.A4]. U.p. konečné pologrupy, která nemá neutrální prvek.

Řešení: $(\{a, b\}, \cdot)$, operaci $\cdot$ definujeme tabulkou

·	a	b
a	a	a
b	a	a

Komentář: Zřejmě se jedná o grupoid, kde platí asociativní zákon, tzn. $(\{a, b\}, \cdot)$ je pologrupa. Přitom pologrupa nemá neutrální prvek e. Kdyby měla, pak by se u tohoto prvku v příslušném řádku opakovalo vodorovné záhlaví tabulky a v příslušném sloupci by se opakovalo svislé záhlaví tabulky.

[**2.1.A5**]. U.p. nekonečné pologrupy, ve které neplatí zákony o krácení.

Řešení: $(\mathbb{Z}, \cdot)$

Komentář: V této pologrupě neplatí zákony o krácení, protože například:
pro $a = 1, b = 2, c = 0$ je $1 \cdot 0 = 2 \cdot 0 \wedge 1 \neq 2$.

[**2.1.A6**]. U.p. pologrupy s jedničkou, v níž k některému prvku existují dva prvky inverzní.

Řešení: Neexistuje.
Protože v pologrupě s jedničkou ke každému prvku existuje nejvýše jeden prvek inverzní.

[**2.1.A7**]. U.p. dvou různých grup tak, že každá z těchto grup má 10 prvků.

Řešení:

- $(G_{10}, \cdot)$, kde $G_{10} = \{z \in \mathbb{C} \mid z^{10} = 1\}$, tzn. G_{10} se sestává ze všech 10-tých odmocnin z 1 v oboru komplexních čísel, operace $\cdot$ značí násobení komplexních čísel

- $(\mathbb{Z}_{10}, +)$, kde $\mathbb{Z}_{10} = \{C_0, C_1, \ldots, C_9\}$, tzn. $\mathbb{Z}_{10}$ je množina všech zbytkových tříd podle modulu 10 a operace $+$ značí sčítání zbytkových tříd podle modulu 10.

[**2.1.A8**]. U.p. dvou nekomutativních grup tak, že jedna je konečná a druhá je nekonečná.

Řešení:

- $A = \{a, b, c\}$
  $G = \{f \mid f : A \to A, f \text{ je bijektivní zobrazení}\}$
  $(G, \circ)$ je nekomutativní konečná grupa

- $G = \{f \mid f : \mathbb{N} \to \mathbb{N}, f \text{ je bijektivní zobrazení}\}$
  $(G, \circ)$ je nekomutativní nekonečná grupa.

Komentář: Skládání zobrazení množiny A do množiny A je typická nekomutativní operace, která je však asociativní. K tomu, abychom dostali grupu, musíme vzít bijektivní zobrazení. Za množinu A vezmeme konečnou množinu (pro vytvoření konečné grupy) nebo nekonečnou množinu (pro vytvoření nekonečné grupy).

[**2.1.A9**]. U.p. pologrupy, ve které platí zákony o dělení a neplatí zákony o krácení.

Řešení: Neexistuje.
Pologrupa ve které platí zákony o dělení je grupa a v každé grupě platí zákony o krácení.

[**2.1.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

c) je nutná a dostatečná

pro to, aby pologrupa $(G, \cdot)$ byla grupou.

Řešení:

a) Pologrupa $(G, \cdot)$ má neutrální prvek.

b) $(G, \cdot) = (\mathbb{Z}, +)$

c) V $(G, \cdot)$ platí zákony o dělení.

§2: PODSTRUKTURY STRUKTUR S JEDNOU OPERACÍ

[**2.2.A1**]. U.p. dvou disjunktních podgrupoidů v grupoidu:

a) $(\mathbb{N}, \cdot)$

b) $(\mathbb{N}, +)$.

Řešení:

a) $(H_1, \cdot)$, $(H_2, \cdot)$, kde $H_1 = \{1\}$, $H_2 = \{2, 4, 6, \dots\}$.

b) Neexistuje.
Dokážeme, že libovolné dva podgrupoidy $(H_1, +)$ a $(H_2, +)$ grupoidu $(\mathbb{N}, +)$ mají vždy neprázdný průnik a to tak, že sestrojíme prvek, který leží v obou grupoidech. Nechť $a \in H_1$ a $b \in H_2$ jsou pevné prvky. Potom (uvědomme si, že násobení přirozench čísel je opakované sčítání)

$$a \cdot b = \underbrace{(b + b + \cdots + b)}_{a\text{-krát}} \in H_1 \ \wedge \ a \cdot b = \underbrace{(a + a + \cdots + a)}_{b\text{-krát}} \in H_1$$

tzn. $a \cdot b \in H_1 \cap H_2$, a tedy $H_1 \cap H_2 \neq \emptyset$.

[**2.2.A2**]. U.p. nekomutativního podgrupoidu v grupoidu $(\mathbb{Z}_{12}, \cdot)$.

Řešení: Neexistuje.
Operace $\cdot$ je komutativní v $\mathbb{Z}_{12}$ a tedy musí být komutativní i v libovolném podgrupoidu grupoidu $(\mathbb{Z}_{12}, \cdot)$.

[**2.2.A3**]. U.p. grupoidu $(G, \cdot)$ s jedničkou e a jeho podgrupoidu $(H, \cdot)$, který

a) nemá jedničku

b) má jedničku, různou od e.

Řešení:

a) $(G, \cdot)$, kde $G = \{e, a, b\}$, $(H, \cdot)$, kde $H = \{a, b\}$ a operace $\cdot$ je definována tabulkou:

·	e	a	b
e	e	a	b
a	a	b	b
b	b	b	b

b) $(G, \cdot)$, kde $G = \{e, a\}$, $(H, \cdot)$, kde $H = \{a\}$ a operace $\cdot$ je definována tabulkou:

·	e	a
e	e	a
a	a	a

Komentář:

a) Zvolme podgrupoid $(H, \cdot)$ tak, aby neobsahoval jedničku. Je vidět, že podgrupoid $(H, \cdot)$ nemůže být jednoprvkový. Tedy množina G musí být alespoň 3-prvková.

b) Zvolme podgrupoid $(H, \cdot)$ tak, aby obsahoval jedničku různou od jedničky grupoidu $(G, \cdot)$. Zde bude nejjednodušší zvolit jednoprvkový podgrupoid. V tomto případě tedy množina G může být 2-prvková.

[**2.2.A4**]. U.p. grupy $(G, \cdot)$ a jejích dvou různých podgrup $(H_1, \cdot)$, $(H_2, \cdot)$ takových, že $(H_1 \cup H_2, \cdot)$

a) není podgrupou v $(G, \cdot)$

b) je podgrupou v $(G, \cdot)$.

Řešení:

a) Grupa $(\mathbb{R} - \{0\}, \cdot)$ a její dvě různé podgrupy $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$.

b) Grupa $(\mathbb{R} - \{0\}, \cdot)$ a její dvě různé podgrupy $(\mathbb{Q}^+ - \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$.

Komentář:

a) Množina $\mathbb{Q} - \{0\} \cup \mathbb{R}^+$ není vzhledem k násobení $\cdot$ ani grupoid. Např.: $\sqrt{2}, -1 \in \mathbb{Q} - \{0\} \cup \mathbb{R}^+$, ale $\sqrt{2} \cdot (-1) = -\sqrt{2} \notin \mathbb{Q} - \{0\} \cup \mathbb{R}^+$.

b) Sjednocením grup $(\mathbb{Q}^+ - \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$ dostaneme grupu $(\mathbb{R}^+, \cdot)$, která je jistě podgrupou grupy $(\mathbb{R}, \cdot)$. Poznamenejme, že lze dokázat, že sjednocení dvou podgrup $(H_1, \cdot)$, $(H_2, \cdot)$ je podgrupou v dané grupě $(G, \cdot)$ právě když jedna podgrupa je podmnožinou druhé tj. $H_1 \subseteq H_2 \vee H_2 \subseteq H_1$.

[**2.2.A5**]. U.p. 17-ti prvkové podgrupy v grupě $(\mathbb{C} - \{0\}, \cdot)$.

Řešení: $(G_n, \cdot)$, kde $G_n = \{z \in \mathbb{C} \mid z^n = 1\}$, tzn. množina G_n se sestává ze všech n-tých odmocnin z 1 v oboru komplexních čísel.

[**2.2.A6**]. Určete všechny podgrupy grupy celých čísel $(\mathbb{Z}, +)$, které obsahují číslo 63.

Řešení:
$(\ 1\cdot\mathbb{Z}, +)$
$(\ 3\cdot\mathbb{Z}, +)$
$(\ 7\cdot\mathbb{Z}, +)$
$(\ 9\cdot\mathbb{Z}, +)$
$(21\cdot\mathbb{Z}, +)$
$(63\cdot\mathbb{Z}, +)$

Komentář: Víme, že $(H, +)$ je podgrupa grupy $(\mathbb{Z}, +)$ právě když existuje celé nezáporné číslo k tak, že $H = k \cdot \mathbb{Z}$. Aby množina H obsahovala číslo 63, musíme k položit rovno přirozenému děliteli čísla 63. Podgrup je pak tolik, kolik je přirozených dělitelů čísla 63 a mají uvedený tvar.

[2.2.A7]. Popište (výčtem prvků) všechny netriviální podgrupy:

a) v grupě $(\mathbb{Z}_{12}, +)$

b) v grupě $(\mathbb{Z}_{13}, +)$.

Řešení:

a) $(H_1, +)$, kde $H_1 = \{C_0, C_2, C_4, C_6, C_8, C_{10}\}$
$(H_2, +)$, kde $H_2 = \{C_0, C_3, C_6, C_9\}$
$(H_3, +)$, kde $H_3 = \{C_0, C_4, C_8\}$
$(H_4, +)$, kde $H_4 = \{C_0, C_6\}$

b) Neexistuje.
V této grupě existují jen triviální podgrupy $(\{C_0\}, +)$, a $(\mathbb{Z}_{13}, +)$, protože přirození dělitelé 13 jsou pouze 1 a 13.

Komentář:

a) Podgrup v grupě $(\mathbb{Z}_m, +)$ je tolik, kolik je přirozených dělitelů čísla m. Do množiny H patří vždy zbytková třída C_0 a další zbytkové třídy, které získáme tak, že k indexu předchozí zbytkové třídy přičítáme přirozeného dělitele k tak dlouho, dokud je to možné.

[2.2.A8]. U.p. netriviální podgrupy v grupě $(\mathbb{Z}_{16}, +)$, která

a) neobsahuje prvek C_8

b) neobsahuje prvek C_2.

Řešení:

a) Neexistuje.
Každé přirozené číslo, které dělí číslo 16 a je menší než 16, musí dělit i číslo 8. Každá podgrupa grupy $(\mathbb{Z}_{16}, +)$ tedy obsahuje prvek C_8.

b) $(H, +)$, kde $H = \{C_0, C_4, C_8, C_{12}\}$.

Komentář:

b) Vybereme podgrupu $(H, +)$, odpovídající přirozenému děliteli k čísla 16, který je větší než číslo 2. Vidíme, že existují 2 možné odpovědi, a to $\{C_0, C_4, C_8, C_{12}\}$ a $\{C_0, C_8\}$.

[2.2.A9]. U.p. přirozeného čísla m tak, aby grupa $(\mathbb{Z}_m, +)$ měla právě

a) 4 podgrupy

b) 5 podgrup

c) k podgrup, kde k je libovolné pevné přirozené číslo.

Řešení:

a) $m = 2^3 = 8$

b) $m = 2^4 = 16$

c) $m = 2^{k-1}$

Komentář: Grupa $(\mathbb{Z}_m, +)$ má tolik podgrup, kolik je přirozených dělitelů čísla m.
Pro případ a) lze za m zvolit i jiná přirozená čísla. Například $m = 6$. Nejjednoduší však je, zvolit m tak, aby bylo mocninou prvočísla.
Pro případ b), kdy počet podgrup je prvočíslo, musíme zvolit m jako čtvrtou mocninu nějakého prvočísla.
Pro vyřešní obecného příkladu c) je vhodné postupovat tak, že za m zvolíme vhodně číslo tak, aby mělo právě požadovaný počet podgrup, tj. za m zvolíme vhodnou mocninu nějakého prvočísla, například čísla 2. Řešení c) je pak zobecněním příkladů a) a b).

[**2.2.A10**]. Nechť $(G, \cdot)$ je grupa; nechť $H \subseteq G$. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

c) je nutná a dostatečná

pro to, aby $(H, \cdot)$ byla podgrupou grupy $(G, \cdot)$.

Řešení:

a) $(H, \cdot)$ je podgrupoid v grupě $(G, \cdot)$.

b) $(H, \cdot) = (2{\cdot}\mathbb{Z}, +), (G, \cdot) = (\mathbb{Z}, +)$.

c) Pro $\forall\, a, b \in H$ platí: $a \cdot b^{-1} \in H$.

§3: STRUKTURY SE DVĚMA OPERACEMI A JEJICH PODSTRUKTURY

[**2.3.A1**]. U.p. okruhu, ve kterém neplatí omezené zákony o krácení.

Řešení: $(\mathbb{Z}_6, +, \cdot)$

Komentář: Víme (viz věta 3.2.), že platnost omezených zákonů o krácení je ekvivalentní neexistenci dělitelů nuly. Jinak řečeno, neplatnost omezených zákonů o krácení je ekvivalentní existenci dělitelů nuly. Stačí tedy uvést příklad okruhu, který má dělitele nuly, např. $(\mathbb{Z}_6, +, \cdot)$.

[**2.3.A2**]. U.p. okruhu, který nemá dělitele nuly a přitom není oborem integrity.

Řešení: $(\{x\}, +, \cdot)$

Komentář: Pokud máme nalézt okruh, který nemá dělitele nuly a přitom není oborem integrity, musíme porušit alespoň jednu ze zbývajících podmínek definice oboru integrity a to buď okruh musí být triviální nebo nekomutativní nebo nesmí mít jedničku. Nejjednodušší je uvážit triviální okruh, ten totiž nemá dělitele nuly a zároveň je porušena definice oboru integrity.

[**2.3.A3**]. U.p. konečného oboru integrity, který není tělesem.

Řešení: Neexistuje.
Podle věty 3.8. je každý konečný obor integrity tělesem.

[**2.3.A4**]. U.p. nenulového prvku v okruhu $(\mathbb{Z}_{17}, +, \cdot)$, k němuž neexistuje prvek inverzní (vzhledem k operaci $\cdot$).

Řešení: Neexistuje
$(\mathbb{Z}_{17}, +, \cdot)$ je obor integrity, protože přirozené číslo 17 je prvočíslo. Zároveň je také konečný obor integrity, protože množina $\mathbb{Z}_{17}$ je konečná. Každý konečný obor integrity je těleso. V tělese však existuje k libovolnému nenulovému prvku existuje prvek inverzní.

[**2.3.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

pro to, aby okruh $(R, +, \cdot)$ byl oborem integrity.

Řešení:

a) $(R, +, \cdot)$ je netriviální okruh.

b) $(R, +, \cdot)$ je těleso.

§4: ČÍSELNÁ TĚLESA

[**2.4.A1**]. U.p. tělesa, které není číselným tělesem.

Řešení: $(\mathbb{Z}_{17}, +, \cdot)$

Komentář: Vybereme takové těleso $(T, +, \cdot)$, kde množina T není podmnožina komplexních čísel.

[**2.4.A2**]. U.p. číselného tělesa, které není oborem integrity.

Řešení: Neexistuje.
Každé těleso, tedy i číselné těleso je vždy obor integrity.

[**2.4.A3**]. U.p. číselného tělesa, které neobsahuje číslo 13.

Řešení: Neexistuje.
Číslo 13 je racionální číslo. Pokud je $(T, +, \cdot)$ číselné těleso, pak T obsahuje množinu $\mathbb{Q}$ všech racionálních čísel (viz věta 3.10.), tedy obsahuje i číslo 13.

[**2.4.A4**]. U.p. číselného tělesa, které neobsahuje číslo $\sqrt{13}$.

Řešení: $(\mathbb{Q}, +, \cdot)$.

Komentář: Zřejmě $(\mathbb{Q}, +, \cdot)$ je číselné těleso. Množina $\mathbb{Q}$ všech racionálních čísel neobsahuje číslo $\sqrt{13}$.

[**2.4.A5**]. U.p. číselného tělesa, různého od $(\mathbb{C}, +, \cdot)$, které obsahuje číslo $(1 + i)$.

Řešení: $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

Komentář: Tento příklad ukazuje, že existují i číselná tělesa různá od tělesa všech komplexních čísel, která se neomezují pouze na reálnou osu (nejsou podmnožinou tělesa všech reálných čísel).

[**2.4.A6**]. Udejte, kolik existuje různých číselných těles.

Řešení: Číselných těles existuje nekonečně mnoho.

Komentář: Například těles tvaru $(\mathbb{Q}(\sqrt{p}), +, \cdot)$, kde p je prvočíslo, je nekonečně mnoho, protože prvočísel je nekonečně mnoho.

[**2.4.A7**]. U.p. číselného tělesa $(T, +, \cdot)$ tak, že platí: $\mathbb{Q} \subset T \subset \mathbb{R}$.

Řešení: $(\mathbb{Q}(\sqrt{2}), +, \cdot)$.

[**2.4.A8**]. U.p. konečného číselného tělesa.

Řešení: Neexistuje.
Všechna číselná tělesa obsahují množinu $\mathbb{Q}$ všech racionálních čísel, která je nekonečná. Proto je každé číselné těleso také nekonečné.

[**2.4.A10**]. U.p. podmínky, která

a) je nutná, ale není dostatečná

b) je dostatečná, ale není nutná

c) je nutná a dostatečná

pro to, aby $(T, +, \cdot)$ bylo číselné těleso.

Řešení:

a) $(T, +)$ je komutativní grupa.

b) $T = \mathbb{Q}$ a operace $+, \cdot$ jsou operace sčítání a násobení čísel.

c) T je alespoň dvouprvková podmnožina množiny $\mathbb{C}$ všech komplexních čísel, uzavřená vzhledem k odečítání čísel a vzhledem k dělení nenulovým číslem.

SEZNAM POUŽITÉ LITERATURY

[1] Horák, P. *Základy matematiky.*
`http://www.math.muni.cz/~horak/zm_2006p.pdf`, 2006.

[2] Horák, P. *Cvičení z algebry a teoretické aritmetiky.*
3. vyd. Brno: Masarykova univerzita, 2006.

[3] Herman, J., Kučera, R., Šimša, J. *Metody řešení matematických úloh I.*
2.vyd. Brno: Masarykova univerzita, 2001.

[4] Pytlíček, J. *Cvičení z algebry a geometrie.*
Praha: Vydavatelství ČVUT, 1998.