Západočeská univerzita v Plzni

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY

ALGEBRAICKÉ STRUKTURY S JEDNOU BINÁRNÍ OPERACÍ A JEJICH ZOBRAZENÍ

BAKALÁŘSKÁ PRÁCE

Marie Černá

Přírodovědná studia, Matematická studia

(2009 – 2012)

Vedoucí práce: *Mgr. Lukáš Honzík*

Plzeň 2012

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, dne…………………..2012

……………………………………………

vlastnoruční podpis

Děkuji vedoucímu bakalářské práce panu Mgr. Lukáši Honzíkovi za odborné vedení, cenné rady, věcné připomínky a trpělivost při vypracování této práce.

Místo pro vložení zadání.

OBSAH

ÚVOD

Pro svou bakalářskou práci jsem si vybrala téma „Algebraické struktury s jednou binární operací a jejich zobrazení“, se kterým jsem se poprvé setkala ve 2. ročníku matematických studií na vysoké škole. Teorie algebraických struktur patří pod algebru, jenž je jednou ze základních matematických disciplín.

Skupina francouzských matematiků vystupujících pod přezdívkou bourbakisté, vyslovují definici „matematika je věda zabývající se vyšetřováním matematických struktur“ a ve svém díle Eléments de mathematique z roku 1939 představují matematiku jako „učení o strukturách“.

Celý text této práce je rozdělen do pěti kapitol. V první se seznámíme se základními pojmy potřebnými ke studiu algebraických struktur, jako jsou množiny, kartézský součin množin, binární relace a zobrazení, které nám pomáhají při objasnění druhé kapitoly o binárních operacích.

Ve třetí kapitole se s binárními operacemi bude pracovat již více, jelikož za jejich pomoci můžeme určit, o jaký typ algebraické struktury se jedná. Postupně si zde probere algebraické struktury s jednou binární operací, jako jsou grupoidy, pologrupy, monoidy a grupy. Uvedeme ke každé z nich základní definice, věty a příklady, které pomohou objasnit danou problematiku.

Ve čtvrté kapitole se poté dostáváme k zobrazení výše uvedených algebraických struktur, k jejich homomorfismu a izomorfismu.

V poslední, páté kapitole se jen zmíníme o existenci algebraických struktur se dvěma binárními operacemi, a uvedeme základní definice každé z nich.

Pokud nebude uvedeno jinak, definice a věty jsou převzaty ze zdrojů, uvedených v seznamu použité literatury.

1. ZÁKLADNÍ POJMY

Pro úspěšné porozumění následujícímu textu zavedeme několik základních pojmů.

1.1. Množina

Jedním z primárních pojmů je pojem **množina**. Pokládáme ji za shrnutí, množství, jakýchsi předmětů, které nazýváme prvky množiny. Jakákoliv množina je svými prvky jednoznačně určena.

Pro rozlišení množin a prvků zavedeme jejich označení. Množiny budeme značit velkými latinskými písmeny, př. K, L, M … a jejich prvky označíme malými latinskými písmeny př. $k, l, m,$ … Obecně můžeme prvky množiny značit i jinak, například čísly, znaky… Je-li prvek k prvkem množiny M, zapisujeme $k \in M$, pokud prvek k nepatří do množiny M, píšeme $k \notin M$. ([1])

Příklady množin:

Množina všech sudých čísel.

Množina všech fialových pastelek v penále.

Množina všech nezáporných čísel od 5 do 86.

Množina všech dívek ve třídě. …

Množinu můžeme zapisovat následujícími metodami:

I. Pokud obsahuje množina konečný počet prvků, hovoříme o udání množiny *výčtem prvků*.

$$K = \{k_1, k_2, k_3, \dots, k_i\},$$

kde $k_1, k_2, k_3, \dots, k_i$ jsou prvky množiny K.

Pokud například množina H obsahuje prvky všechny sudá čísla od 2 do 20, zapisujeme $H = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$.

Výčty prvků mohou být zadány jako kompletní nebo nekompletní, přičemž kompletní lze uplatnit u množin majících rozumný nízký počet prvků, např.

[1] Ekvivalentní zápisy k „$k \in M$“ a „$k \notin M$“ jsou zápisy „$M \ni k$“ a „$M \not\ni k$“

všechna celá čísla od 1 do 5 – $\{1;\ 2;\ 3;\ 4;\ 5\}$, zatímco u množin s vyšším konečným počtem prvků, u nichž to jde díky nějaké pravidelnosti, je nutné výčet prvků zkrátit, např. všechny násobky čísla 5 od 0 do 100 – $\{0; 5; 10; 15; \dots ; 100\}$. Částečně odkazujeme na nějakou charakteristickou vlastnost prvků, i když není přímo pojmenovaná.

II. Množinu můžeme zapsat *charakteristickou vlastností prvků*. Jedním z důvodů může být nekonečnost množiny.

$$K = \{k; Z(k)\},$$

kde k jsou prvky množiny K, udávané vlastností $Z(k)$.

Máme-li množinu J, která obsahuje prvky j a obsahuje reálná čísla na intervalu $\langle 0; 3\rangle$, píšeme

$$J = \{j \in R; \langle 0; 3\rangle\}.$$

III. Množinu zapisujeme *určením prvního prvku*, pokud jsou prvky množiny tvořeny členy nějaké posloupnosti.

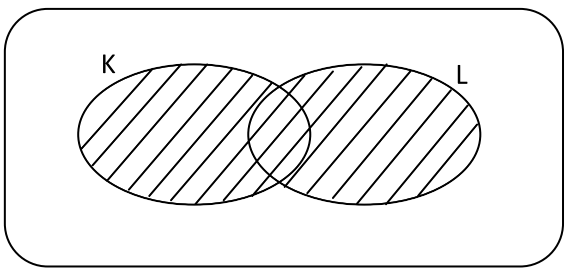
Základní operace s množinami:

Mějme dvě libovolné množiny K, L. Potom na těchto dvou množinách definujeme:

I. *sjednocení množin*, pokud existují prvky, které jsou obsaženy alespoň v jedné z obou množin.

$$K \cup L = \{k; k \in K \vee k \in L\}$$

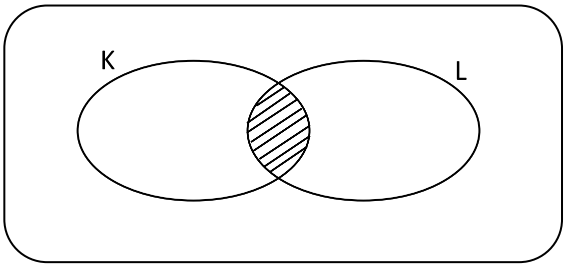
Grafické znázornění:



II. *průnik množin*, pokud existují prvky, které se vyskytují v obou množinách zároveň

$$K \cap L = \{k; k \in K \wedge k \in L\}$$

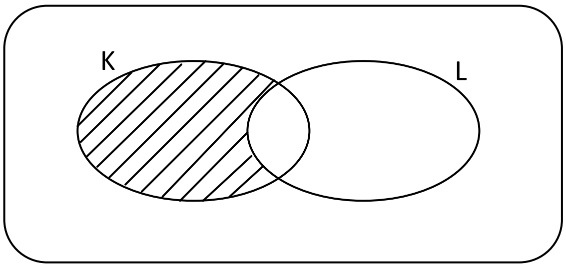
Grafické znázornění:



III. *rozdíl množin*, pokud existují prvky, které se vyskytují v množině K a nejsou prvky z množiny L

$$K \setminus L = \{k; k \in K \wedge k \notin L\}$$

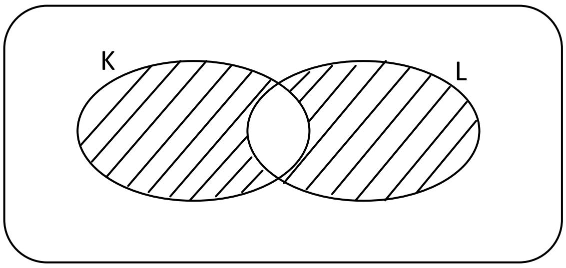
Grafické znázornění:



IV. *symetrický rozdíl množin*, pokud obsahuje prvky, které patří právě do jedné z množin K, L, ale nejsou prvky obou množin současně

$$K \,\Delta\, L = \left\{k; k \in K \;\underline{\vee}\; k \in L\right\}$$

Grafické znázornění:



Příklad 1. – Máme množinu $H = \{1,2,3,4,5,6\}$ a množinu $I = \{2,4,6,8\}$. Určete sjednocení, průnik, rozdíl $H \setminus I$ a symetrický rozdíl množin $H \,\Delta\, I$.

Řešení:

Sjednocením množin H, I jsou všechny prvky, které se vyskytují v množině H nebo v množině I.

Tedy

$$H \cup I = \{1, 2, 3, 4, 5, 6, 8\}.$$

Průnikem množin H, I jsou prvky, které náleží do obou množin zároveň. Jedná se tedy o prvky

$$H \cap I = \{2, 4, 6\}.$$

Rozdílem množin $H \setminus I$ rozumíme prvky, které jsou z jedné množiny a nejsou prvky množiny druhé. Jedná se tedy v našem případě o prvky

$$H \setminus I = \{1, 3, 5\}.$$

Symetrickým rozdílem množin $H \,\Delta\, I$ jsou prvky obou množin, kromě prvků, které jsou pro obě společné. V našem případě tedy

$$H \,\Delta\, I = \{1, 3, 5, 8\}.$$

1.2. Kartézský součin množin

V matematice pracujeme častokrát s dvojicemi prvků, kde umíme určit jejich pořadí. Tyto prvky nazýváme uspořádané dvojice, je-li prvků více, jedná se o uspořádané k-tice. Tyto uspořádané k-tice budeme zapisovat výčtem prvků $(n_1, n_{2,} \dots n_k)$.

Množinu $K \times L$, kde K a L jsou dvě libovolné množiny a platí

$$K \times L = \{(x, y); x \in K \ \wedge \ y \in L\},$$

nazýváme **kartézským součinem množin**.

Příklad 2. – Mějme dvě množiny $U = \{s, t, 4\}, V = \{y, z\}$. Určete kartézský součin těchto dvou množin.

Řešení:

$$U \times V = \{(s, y); (s, z); (t, y); (t, z); (4, y); (4, z)\}.$$

1.3. Binární relace

Libovolnou množinu R, která je podmnožinou kartézského součinu $K \times K$, nazveme **binární relací** na množině K.

Vlastnosti binárních relací:

Binární relace R definovaná na množině K se nazývá:

i) **reflexivní**, pokud $\forall\ x \in K$ platí $[x, x] \in R$

ii) **areflexivní,** pokud $\exists\ x \in K$ platí $[x, x] \notin R$

iii) **antireflexivní**, za podmínky že $\forall\ x \in K$ platí $[x, x] \notin R$

iv) **symetrická**, jestliže $\forall\ x, y \in K$ platí $[x, y] \in R \Rightarrow [y, x] \in R$

v) **antisymetrická**, jestliže $\forall\ x, y \in K$ platí $[x, y] \in R \Rightarrow [y, x] \notin R$

vi) **asymetrická,** za podmínky, že $\forall\ x, y \in K$ platí $[x, y] \in R \wedge [y, x] \in R \Rightarrow x = y$

vii) **tranzitivní**, pokud $\forall\ x, y \in K$ platí $[x, y] \in R\ \wedge\ [y, z] \in R \Rightarrow [x, z] \in R$.

Pokud je relace R definovaná na množině K současně reflexivní, symetrická a tranzitivní, hovoříme o **relaci ekvivalence.** V případě, že je relace reflexivní, antisymetrická a tranzitivní, jedná se o **relaci uspořádání.**

Příklad 3. – Je dána množina $K = \{a, b, c, d, e, f\}$ a v ní relace $A = \{(c, a), (b, e), (a, c), (d, d), (e, e), (f, f), (b, f), (d, f), (b, b), (f, d)\}$. Rozhodněte, zda relace A je relací ekvivalence.

Řešení:

Relace je areflexivní, jelikož $a, c \in K$, a přesto $(a, a) \notin A$ a též $(c, c) \notin A$. Antisymetrická, protože $(b, e) \in A$, ale zároveň $(e, b) \notin A$, totéž platí u dvojice $(b, f) \in A$, ale zároveň $(f, b) \notin A$. Není tranzitivní, protože například platí $(b, f) \in A\ \wedge\ (f, d) \in A$, avšak $(b, d) \notin A$. Docházíme tedy k závěru, že se nejedná o relaci ekvivalence.

Příklad 4. – Je dána množina $L = \{2, 3,7\}$ a v ní relace $B = \{(2,2), (7,2), (3,2), (3,3), (2,3), (2,7), (3,7), (7,7), (7,3)\}$. Rozhodněte, zda relace B je relací ekvivalence.

Řešení:

Relace je reflexivní, protože pro všechny tři prvky množiny L platí, že jsou v relaci samy se sebou, tj. $(2,2) \in B, (3,3) \in B, (7,7) \in B$. Symetrická, protože pro všechny dvojice prvků (x, y), pro $x, y \in L$, které jsou spolu v relaci s B, platí, že i dvojice (y, x) patří do relace B. Tranzitivní, jelikož relace B obsahuje všechny uspořádané dvojice (x, y), pro $x, y \in L$, z čehož plyne, že vždy bude platit $(x, y) \in B \ \wedge \ (y, z) \in B \Rightarrow (x, z) \in B$.

U tohoto případu docházíme k závěru, že se jedná o relaci ekvivalence.

1.4. Zobrazení

Zobrazením množiny $\boldsymbol{K}$ do množiny $\boldsymbol{L}$, budeme uvažovat binární relaci ω mezi množinami K a L, pro kterou platí:

i) $\forall x \in K \ \exists y \in L\colon \ [x, y] \in \gamma$

ii) $\forall x \in K \ \forall y_1, y_2 \in L\colon [x, y_1] \in \gamma \wedge [x, y_2] \in \gamma \Longrightarrow y_1 = y_2$

Z těchto dvou výše uvedených podmínek můžeme vytvořit jednu, pro kterou platí:

$$\forall x \in K \ \exists!\, y \in L\colon [x, y] \in \gamma$$

Zobrazení můžeme rozdělit:

I. Řekneme, že zobrazení $\gamma\colon K \to L$ se nazývá *surjektivní*, jestliže platí
$$\gamma(K) = L$$

II. O zobrazení $\gamma\colon K \to L$ hovoříme jako o *injektivním*, jestliže platí
$$\forall x, z \in K\colon \gamma(x) \neq \gamma(z) \Longrightarrow x \neq z$$

III. Řekneme, že zobrazení $\gamma\colon K \to L$ se nazývá *bijektivní*, jestliže je surjektivní a zároveň také injektivní.

Příklad 5. – Je dáno, že $\forall x \in Z\colon f(x) = x^2 + 2x + 6, f(x) \in Z$. Rozhodněte, zda se jedná o bijektivní zobrazení.

Řešení:

Zobrazení $f(x) = x^2 + 2x + 6$ není injektivní, protože například pro $x_1 = 0$ a $x_2 = -2$ (kde $x_1 \neq x_2$), platí $f(x_1) = 6$ a $f(x_2) = 6$, tedy není splněna nerovnost $f(x_1) \neq f(x_2)$. Není surjektivní proto, že na množinu obrazů není celá množina celých čísel, jinými slovy prvky $\{\dots, -2, -1, 0\} \subset Z$ nemají v množině vzorů svůj vzor. Z neplatnosti injekce a neplatnosti surjekce dostáváme závěr, že zobrazení není bijektivní.

2. Binární operace

Definice 2. 1. – Kterékoliv zobrazení kartézského součinu $\mathrm{K} \times \mathrm{K}$ do množiny K definované na libovolné neprázdné množině K se nazývá **binární operací.**

$$\circ : K \times K \to K$$

Pro označování binárních operací můžeme používat mnoha značení př. $\blacksquare, \circ, \ *, \circ, \Delta$ ... Pro tuto práci budu používat označení $\circ$.

Jako příklad binární operace můžeme uvést základní aritmetické operace sčítání a násobení čísel.

Praktická ukázka binární operace sčítání:

$$5 + 7 = 13$$

lze zapsat: $[5,7] \xrightarrow{+} 13$ nebo $+ : [5,7] \to 13$.

Základní vlastnosti binárních operace

Definice 2. 2. – Nechť máme neprázdnou množinu K. Potom binární operaci $\circ$, pro kterou platí

$$\forall\, k, l \in K: \quad k \circ l = l \circ k,$$

nazýváme *komutativní.*

Pro komutativní operaci tedy platí, že můžeme zaměnit pořadí prvků, aniž by se změnil výsledek.

Pro příklad uvedeme pár komutativních binárních operací: numerický operace sčítání a násobení na množinách všech přirozených čísel kromě nuly (N), celých čísel (Z), racionálních čísel (Q), reálných (R) a komplexních čísel (C); sčítání vektorů; sčítání matic, operace s množinami při sjednocení a průniku.

$3 + 2 = 5 = 2 + 3,$ … jedná se o komutativní operace

$10 - 6 = 4 \neq 6 - 10 = -4,$ … není komutativní operací

Za komutativní operaci nelze považovat například numerické odčítání a dělení, násobení matic.

Definice 2. 3. – Nechť máme neprázdnou množinu K. Potom binární operaci ○, pro kterou platí

$$\forall\, k, l, m \in K\colon (k \circ l) \circ m = k \circ (l \circ m),$$

nazýváme *asociativní*.

Pro asociativní operaci tedy platí, že uzávorkování nehraje roli při konečném výsledku.

Příklad některých asociativních operací: numerický operace sčítání a násobení na množinách všech přirozených čísel kromě nuly (N), celých čísel (Z), racionálních čísel (Q), reálných (R) a komplexních čísel (C). Opět operace numerické odčítání a dělení nelze považovat za asociativní operace na množině K.

$(4 + 6) + 10 = 20 = 4 + (6 + 10),$ … jedná se o asociativní operace

$(40/5)/2 = 4 \neq 40/(5/2) = 16,$ … není asociativní operací

Definice 2. 4. – Nechť máme neprázdnou množinu K. Potom binární operaci ○, kde existuje prvek $e \in K$, pro který platí

$$\forall k \in K\colon e \circ k = k \circ e = k$$

nazveme operací s *neutrálním prvkem*.

V případě, že platí pouze

$$\forall k \in K\colon e \circ k = k,$$

hovoříme o binární operaci ○ s *levým neutrálním prvkem*.

Jestliže

$$\forall k \in K\colon k \circ e = k,$$

potom hovoříme o binární operaci ○ s *pravým neutrálním prvkem*.

Věta 1. – V každé binární operaci $\circ$ se vyskytuje nanejvýše jeden neutrální prvek.

Důkaz: Mějme binární operaci $\circ$ s neutrálními prvky e a e', kde $e \neq e'$. Jestliže $e \circ e' = e'$ a současně $e \circ e' =$ e, potom pokud se rovnají levé strany obou rovností, musí se rovnat i pravé strany, tedy $e = e'$. V rovnosti $e = e'$ docházíme ke sporu, a tudíž nemůže existovat více jak jeden neutrální prvek.

Příklady některých binárních operací s neutrálním prvkem:

Sčítání na množinách Z, Q, R a C s nulou: $5 + 0 = \mathbf{5} = 0 + 5$

Násobení konstanty jedničkou: $7.1 = \mathbf{7} = 1.7$

Sčítání matice s nulovou maticí: $\begin{pmatrix} 5 & 9 \\ 7 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{5} & \mathbf{9} \\ \mathbf{7} & \mathbf{2} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 5 & 9 \\ 7 & 2 \end{pmatrix}$

Násobení matic maticí jednotkovou. $\begin{pmatrix} 5 & 9 \\ 7 & 2 \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{5} & \mathbf{9} \\ \mathbf{7} & \mathbf{2} \end{pmatrix}$

Sčítání vektoru s vektorem nulovým. $\vec{u} + \vec{o} = \vec{u}$

Příklady s jednostranným neutrálním prvkem.

Pravý neutrální prvek operace odčítání je nula: $7 - 0 = 7$

Pravý neutrální prvek operace dělení je jedna: $\frac{4}{1} = 4$

Definice 2. 5. – Nechť máme neprázdnou množinu K, potom binární operaci $\circ$, kde existuje prvek $a \in K$, pro který platí

$$\forall k \in K: a \circ k = k \circ a = a$$

nazveme operací s agresivním prvkem.

Stejně jako u neutrálního prvku, můžeme hovořit o pravém nebo levém agresivním prvku.

Příklad binární operace s agresivním prvkem:

Násobení konstanty (nulové matice) nulou.

Definice 2. 6. – Nechť máme neprázdnou množinu K s neutrálním prvkem $e \in K$. Potom pro prvek $k \in K$ v binární operaci $\circ$ existují prvky $k^{-1} \in K$, které se nazývájí *inverzními prvky*, pokud

$$k \circ k^{-1} = k^{-1} \circ k = e.$$

Pro příklad uvedeme některé operace s inverzními prvky:

Sčítání celých čísel. Máme-li nenulové celé číslo k a k němu číslo opačné $(-k)$. Potom pro součet těchto dvou čísel platí: $k + (-k) = 0$

$$6 + (-6) = 0.$$

Násobení nenulových reálných čísel. Máme-li nenulové reálné číslo k a k němu číslo převrácené $\frac{1}{k}$. Potom pro násobek těchto dvou čísel platí: $k \,.\frac{1}{k} = 1$. Inverzním prvkem této

$$5 \,.\, \frac{1}{5} = 1.$$

Sčítání matic. Máme-li matici A a k ní opačnou matici $(-A)$. Potom pro součet těchto dvou matic platí: $A + (-A) = O$, kde O je nulová matice.

Z předchozí definice však nelze jednoznačně určit, zda existují inverzní prvky v dané operaci.

Věta 2. – Pokud pro neprázdnou množinu K, kde existuje neutrální prvek e, binární operace $\circ$ je asociativní, potom k prvku $k \in K$ existuje maximálně jeden inverzní prvek.

Důkaz: Nechť a^{-1} a b^{-1} jsou inverzní prvky k prvku $k \in K$ a e je neutrální prvek. Potom dle definice o asociativitě, definice o neutrálním prvku a definice o inverzním prvku určíme

$$a^{-1} = a^{-1} \circ \mathrm{e} = a^{-1} \circ (k \circ b^{-1}) = (a^{-1} \circ k) \circ \mathrm{b}^{-1} = e \circ b^{-1} = \mathrm{b}^{-1},$$

z čehož vyplývá $a^{-1} = b^{-1}$. Tudíž se jedná pouze o jeden inverzní prvek.

Příklad 6: Vyšetřete základní vlastnosti pro binární operaci $\circ$ definovanou na množině K, pokud $k \circ l = \frac{k+l}{3}$.

Určíme vlastnosti:

a) *Komutativita:* $k \circ l = l \circ k$:

$k \circ l = \frac{k+l}{3} = \frac{l+k}{3} = l \circ k$ je splněna

b) *Asociativita:* - předpokládáme rovnost pravé a levé strany

$$(k \circ l) \circ m = k \circ (l \circ m)$$

$$(k \circ l) \circ m = \frac{\frac{k+l}{3} + m}{3} = \frac{k + \frac{l+m}{3}}{3} = k \circ (l \circ m)$$

$$\frac{\frac{k+l}{3} + m}{3} = \frac{k + \frac{l+m}{3}}{3}$$

$$\frac{1}{9}k + \frac{1}{9}l + \frac{1}{3}m = \frac{1}{3}k + \frac{1}{9}l + \frac{1}{9}m$$

$$k + l + 3m = 3k + l + m$$

$$2m = 2k$$

$$m = k$$

Není asociativní, tudíž záleží na uzávorkování. V případě, že by $m = k$, potom by v této operaci nezáleželo na uzávorkování.

c) *Existence neutrálního prvku:* $k \circ e = e \circ k = k$

$$k \circ e = \frac{k+e}{3} = k$$

$$k + e = 3k$$

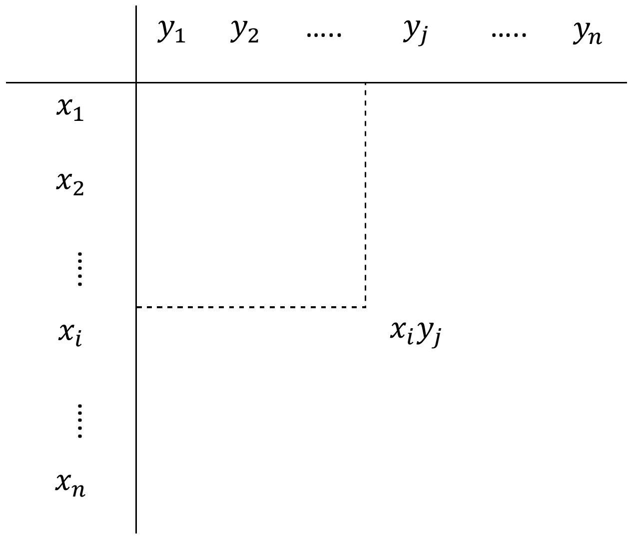
$$e = 2k$$

Neexistuje neutrální prvek. Jelikož neexistuje neutrální prvek, není potřeba hledat prvek inverzní, jelikož taky neexistuje.

Zjištění vlastností binárních operací pomocí multiplikativní tabulky

Pokud máme n-prvkovou konečnou množinu $K = \{1, 2, 3, \dots n\}, kde\ n \geq 1$, můžeme pro zápis binárních operací na množině K užívat tzv. *operativní* neboli *Cayleyho tabulku.* Tabulku sestavíme následovně: do záhlaví řádků a sloupců zapisujeme zpravidla prvky množiny K v identickém pořadí, které od ostatních oddělujeme plnou čarou. Stejné pořadí prvků nám usnadní zjišťování základních vlastností množiny. Výsledek operace $x_i y_j$ musí být uveden v příslušném i. řádku a j. sloupci.

Obrázek:



Jak zjistit binární operace z tabulky si ukážeme na následujícím příkladu:

Příklad 7: Na množině $B = \{0, 1, 2, 3\}$ vyšetřete binární operaci $\circ$ definovanou takto,

$$b \circ c = (b + c)\ (modulo\ 4).$$

$\circ$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

1) **Vyšetříme komutativnost**
Pokud jsou hodnoty tabulky symetrické podle hlavní diagonály, můžeme hovořit o komutativní binární operaci $\circ$.
V našem případě je operace sčítání na množině B komutativní.
2) **Asociativnost** nelze jednoznačně určit z tabulky.
Přesto ale víme, že operace sčítání je asociativní
$$(b + c) + d = b + (c + d) = b + c + d,$$
jelikož při sčítání nezáleží na uzávorkování. Asociativnost se nezmění ani za provedení operace modulo.
3) **Existence neutrálního prvku**
Pravý neutrální prvek – pokud je totožný řádek vedle e se svislým záhlavím tabulky.
Levý neutrální prvek – pokud je totožný sloupec pod e s vodorovným záhlavím

tabulky. Vzhledem k tomu, že existuje jak levý, tak pravý neutrální prvek a tyto prvky jsou si rovny, existuje neutrální prvek a je jím 0.

4) Existence inverzního prvku

Inverzní prvky jsou k sobě ty prvky, které v dané binární operaci dávají výsledek rovný neutrálnímu prvku, neboli hledáme v tabulce výskyty neutrálního prvku, kde ho najdeme, tam jsou k sobě příslušné prvky v záhlaví sloupců a řádek navzájem inverzní Pokud existuje ke každému prvku prvek opačný.

Pro inverzní prvky tedy platí: $-0 = 0, -1 = 3, -2 = 2, -3 = 1.$

3. Algebraické struktury s jednou binární operací

Definice 3. 1. – Mějme neprázdnou množinu K, na které je definována alespoň jedna binární operace. Potom hovoříme o algebraických strukturách s binárními operacemi. Množinu K můžeme označit také jako nosič algebraické struktury.

Je-li na množině K definována binární operace $\circ$, potom hovoříme o algebraické struktuře s jednou binární operací $(K, \circ)$.

Příklady algebraických struktur s jednou binární operací:

Grupoid, pologrupa, monoid, grupa, Abelův grupoid (pologrupa, monoid, grupa).

Grupoid

Definice 3. 2. 1. – Nechť máme neprázdnou množinu K a v ní neomezeně definovanou binární operaci $\circ$, potom dvojice $(K, \circ)$ se nazývá *grupoid*.

V případě, že $\forall k, l \in K: k \circ l = l \circ k$, hovoříme o *komutativním grupoidu* nebo také *Abelově*.

Poznámka: Abelův dostal svůj název podle matematika Nielse Henrika Abela (1802-1829)

Za příklady grupoidů můžeme uvést například: $(N, +), (Z, +), (N, *)$, kde operace $+$, $*$ reprezentují sčítání a násobení.

Věta 3. – Existuje-li grupoid $K = (K, \circ)$, potom existuje v K nanejvýš jedna jednotka.

Důkaz: Mějme m, n, dvě jednotky v K, potom pro ně platí $m = m \circ \mathrm{n} = n$, platí tedy, že jsou stejné $m = n$, proto také hovoříme pouze o jedné jednotce.

Příklad: Mějme množinu všech celých čísel Z a na ní definovanou binární operaci sčítání $+$. Dvojici $(Z, +)$ nazveme grupoid. Je jednoznačné, že pro tento grupoid existuje jednička. Je jí číslo nula, kde $d + 0 = d = 0 + d$, $\forall d \in Z$.

Definice 3. 2. 2. - Existuje grupoid $K = (K, \circ)$. Existuje také $P \neq \emptyset \ \wedge P \subseteq K$. Potom označíme dvojici $(P, \circ)$ *podgrupoidem grupoidu* K, pokud pro všechna p, q z množiny P platí $p \circ q \in P$,

$$(P, \circ) \subseteq (K, \circ).$$

Z této definici odvodíme i následující větu:

Věta 4. - Existuje grupoid $K = (K, \circ)$ a $\{P_1, P_2 \dots P_i\}$, kde $i \in I$, je systém jeho podgrupoidů. Potom průnik $\{P_1 \cap P_2 \cap \dots P_i\}$ systému jeho podgrupoidů je buď podgrupoid v množině K nebo prázdná množina.

Důkaz: Mějme $H = \{P_1 \cap P_2 \cap \dots P_i\}$ kde $i \in I$. H není neprázdná množina. Je-li $h, j \in \{P_1, P_2 \dots P_i\}$, potom je i $h, j \in H$ a platí $h \circ j \in \{P_1, P_2 \dots P_i\}$. Z toho plyne, že $h \circ j \in H$, a tudíž i H je podgrupoid grupoidu K.

Definice 3. 2. 3. - Existuje grupoid $K = (K, \circ)$ a platí pro něj $T \neq \emptyset \ \wedge T \subseteq K$. Potom množinu T obsaženou v průniku všech podgrupoidů grupoidu K označujeme jako *podgrupoid grupoidu* K *generovaný množinou* T (označujeme jako $[T]$) *Množinou generátorů* grupoidu $[T]$ pak nazýváme množinu T.

Uvedeme si jednoduchý příklad na ukázku tohoto typu algebraické struktury:

Příklad 8. – Vzorový příklad na vyšetření algebraické struktury zvané grupoid. Mějme množinu

$$M = Z, k \,\Delta\, l = k - l, \qquad \forall k, l \in M,$$

kde Z je množina celých čísel.

Řešení:

Nejdříve si určíme, zda je tato operace uzavřená na množině Z.

Odečtením jednoho celého čísla od druhého dostaneme opět nějaké celé číslo.

$$k - l = m, \qquad \forall k, l, m \in Z$$

Vyšetříme komutativnost:

$$k \,\Delta\, l = k - l \neq l - k = l \,\Delta\, k$$

Při odčítání docházíme k tomu, že daná struktura není komutativní. Dostávaná algebraickou strukturu zvanou grupoid. Protože není komutativní, nemůžeme hovořit o Abelově grupoidu.

Pologrupa

Definice 3. 3. 1. – Nechť máme neprázdnou množinu L a v ní definovanou binární operaci $\circ$, potom dvojici $(L, \circ)$ nazýváme *pologrupou*, jestliže

$$\forall\, k, l, m \in L: (k \circ l) \circ m = k \circ (l \circ m) \qquad \text{je asociativní.}$$

Pokud pro pologrupu platí $\forall k, l \in L: k \circ l = l \circ k$, hovoříme o *komutativní pologrupě*, nebo také *Abelově*.

Příklady pologrup: $(N, +), (Z, +), (N, *)$, kde operace $+$, $*$ reprezentují sčítání a násobení. Za pologrupu nepovažujeme dvojici $(Z, -)$, kde – je operace odčítání.

Pokud je splněna asociativnost, potom už nám nezáleží na uzávorkování, pokud jsou prvky uvedeny ve stejném pořadí. Můžeme tedy pro pologrupy uvádět $(k \circ l) \circ m = k \circ (l \circ m) = k \circ l \circ m$. Tento předpis můžeme rozšířit i pro libovolnou n-tici prvků $k_1, k_{2,} \dots k_n \in L$, kde $n \geq 3$.

Věta 5. – Mějme pologrupu $(L, \circ)$ s prvky $k_1, k_{2,} \dots k_n \in L$, kde $n \geq 3$. Potom u všech prvků uvedených ve stejném pořadí pro uzávorkování při provedení operace $\circ$ získáme stejný konečný prvek.

Důkaz: Dokážeme si, že pro jakékoliv uzávorkování je konečný prvek stejný jako prvek $k_1 \circ k_2 \circ \dots \circ k_n$, pro $n > 3$.

Máme prvky $k_1, k_{2,} \dots k_n \in L$, pro které

$$k_1 \circ k_2 \circ \dots \circ k_n = (\dots((k_1 \circ k_2) \circ k_3) \circ k_4) \circ \dots) \circ k_n$$

Mějme $v = v_1 \circ v_2$, jako součin prvků $k_1, k_{2,} \dots k_n \in L$. Určíme si dále dvě možnosti, které mohou vzniknout za pomoci matematické indukce:

I) Za indukčního předpokladu platí $v_1 = k_1 \circ k_2 \circ \dots \circ k_{n-1}$, pokud $v_2 = k_n$. A píšeme $v = (k_1 \circ k_2 \circ \dots \circ k_{n-1}) \circ k_n = k_1 \circ k_2 \circ \dots \circ k_{n-1} \circ k_n$,

II) Podle indukčního předpokladu kde $1 \geq h \geq n-2$, platí

$$v_1 = k_1 \circ k_2 \circ \dots \circ k_h, \;\; v_2 = k_{h+1} \circ \dots \circ k_n$$

pokud $v_2$vzniklo vynásobením nejméně 2 prvků.

Nyní tedy dostáváme:

$$\begin{aligned} v = (k_1 \circ k_2 \circ \dots \circ k_h) \circ (k_{h+1} \circ \dots \circ k_{n-1} \circ k_n) \\ &= (k_1 \circ k_2 \circ \dots \circ k_h) \circ ((k_{h+1} \circ \dots \circ k_{n-1}) \circ k_n) \\ &= ((k_1 \circ k_2 \circ \dots \circ k_h) \circ (k_{h+1} \circ \dots \circ k_{n-1})) \circ k_n \\ &= (k_1 \circ k_2 \circ \dots \circ k_{n-1}) \circ k_n = k_1 \circ k_2 \circ \dots \circ k_{n-1} \circ k_n. \end{aligned}$$

Docházíme k závěru, že při dodržení stejného pořadí prvků při provedení operace $\circ$ nezáleží na uzávorkování. [12]

Definice 3. 3. 2. - Pologrupu $(L, \circ)$, kde existuje prvek $k \in L$ a m je přirozené číslo, budeme nazývat jako m-tou přirozenou mocninu prvku k, kde $k^m \in L$, pro které platí

$$k^1 = k; k^{m+1} = k^m \circ k.$$

Věta 6. – Pro kladná přirozená čísla k, l, kde pokud existují libovolné prvky f, g definované jako prvky pologrupy $(L, \circ)$, kde $f \circ g = g \circ f$, platí:

i. $f^k \circ f^l = f^{k+l}$

ii. $(f^k)^l = f^{kl}$

iii. $(f \circ g)^l = f^l \circ g^l$

Důkaz: Použijeme matematické indukci k důkazu uvedených rovností.

i. Je-li

$$\forall l = 0: f^k \circ f^0 = f^k \circ 1 = f^{k+0} = f^k,$$

$$\forall l = 1: \quad f^k \circ f^1 = f^k \circ f = \; f^{k+1},$$

$\forall\, l = m$: $f^k \circ f^m = f^{k+m}$, a nyní dokážeme, pokud

$$\forall l = m+1: \; f^k \circ f^{m+1} = f^k \circ (f^m \circ f) = (f^k \circ f^m) \circ f = f^{k+m} \circ f = f^{k+m+1}$$

ii.

$$\forall\ l = 1: (f^k)^1 = f^k = f^{k.1}$$

$\forall\ l = m: (f^k)^m = f^{km}$, a nyní dokážeme, pokud

$$\forall l = m + 1: (f^k)^{m+1} = (f^k)^m \circ f^k = f^{km} \circ f^k = f^{km+k} = f^{k(m+1)}$$

iii.

$$\forall\ l = 1: (f \circ g)^1 = f^1 \circ g^1 = f^1 \circ g^1 = f\ \circ g$$

$\forall\ l = m: (f \circ g)^m = f^m \circ g^m$, a nyní dokážeme, pokud

$$\forall l = m + 1: (f \circ g)^{m+1} = (f\ \circ g)^m \circ (f \circ g) = f^m \circ g^m \circ f \circ g = f^{m+1} \circ g^{m+1}$$

Definice 3. 3. 3. – Mějme pologrupu $L = (L, \circ)$ a podgrupoid množiny $L, H = (H, \circ)$. Potom hovoříme o H jako o podpologrupě pologrupy L.

Uvedeme si jednoduchý příklad na ukázku tohoto typu algebraické struktury:

Příklad 9. – Vzorový příklad na vyšetření algebraické struktury zvané pologrupa. Mějme množinu

$$M = Z_S, \qquad k\ \Delta\ l = k \cdot l, \qquad \forall k, l \in M,$$

kde Z_S je množina sudých celých čísel.

Řešení:

Nejdříve si určíme, zda je tato operace uzavřená na množině Z_S.

Ze součinu dvou sudých čísel lze vždy vytknout číslo 2 a tudíž i výsledek je sudý.

$$4 * 8 = (2 * 2) * (2 * 4)$$

I. Vyšetření komutativnosti:

$$k\ \Delta\ l = l\ \Delta\ k$$
$$k \cdot l = l \cdot k$$

Vycházíme z toho, že pro sudá celá čísla, je operace násobení komutativní.

II. Vyšetření asociativnosti:

$$(k\ \Delta\ l) \Delta\ m = k\ \Delta\ (l\ \Delta\ m)$$

$$(k \cdot l) \cdot m = k \cdot (l \cdot m)$$

Vidíme, že operace násobení sudých celých čísel je asociativní.

Tudíž naše vyšetřovaná algebraická struktura se nazývá pologrupa. Jelikož je ještě komutativní, můžeme říct, že jde o Abelovu pologrupu.

Monoid

Definice 3. 4. – Nechť máme neprázdnou množinu M a na ní definovanou binární operaci $\circ$, potom dvojici $(M, \circ)$ nazýváme *monoid*, jestliže

$\forall\, k, l, m \in M: (k \circ l) \circ m = k \circ (l \circ m)$ je asociativní,

$\exists e \in M\ \forall k \in M: e \circ k = k \circ e = k$ existuje neutrální prvek.

Pokud je dále monoid, kde $\forall k, l \in M: k \circ l = l \circ k$, komutativní, hovoříme o *komutativním monoidu*, nebo také *Abelově*.

Příklady monoidů: $(N_0, +), (N,\ \cdot), (R,\ \cdot)$. Za monoid nelze považovat $(N, +)$, neboť algebraická struktura neobsahuje neutrální prvek.

I pro tento typ algebraické struktury si uvedeme jednoduchý příklad:

Příklad 10. – Vzorový příklad na vyšetření algebraické struktury monoid. Mějme množinu

$$M = R, k \,\Delta\, l = k - k \cdot l + l$$

kde R jsou všechna reálná čísla.

Řešení:

Nejdříve si určíme, zda je tato operace uzavřená na množině R.

Od reálného čísla odečíst součin dvou reálných čísel a poté přičíst reálné číslo, nám opět udává reálné číslo.

I. Vyšetření komutativnosti:

$$k \,\Delta\, l = l \,\Delta\, k$$

$$k - k \cdot l + l = l - l \cdot k + k$$

$$0 = 0$$

Operace je komutativní

II. Vyšetření asociativnosti:

$$(k \,\Delta\, l) \Delta\, m = k \,\Delta\, (l \,\Delta\, m)$$

$$(k - k \cdot l + l) \,\Delta\, m = k \,\Delta\, (l - l \cdot m + m)$$

$$(k - k \cdot l + l) - (k - k \cdot l + l) \cdot m \; + m = k - k \cdot (l - l \cdot m + m) + (l - l \cdot m + m)$$

$$k - k \cdot l + l - k \cdot m + k \cdot l \cdot m - l \cdot m + m = k - k \cdot l + k \cdot l \cdot m - k \cdot m + l - l \cdot m + m$$

$$0 = 0$$

Operace je asociativní.

III. Vyšetření existence neutrálního prvku:

$$k \,\Delta\, e = e \,\Delta\, k = k.$$

Vyšetříme zvlášť pravý a levý neutrální prvek:

$$P\!: \; k - k \cdot e + e = k$$
$$L\!: \; e - e \cdot k + k = k$$

Existuje neutrální prvek $e = 0$.

Tudíž se jedná o monoid. Jelikož platila komutativnost operace, můžeme označit tuto strukturu jako Abelův monoid.

Grupa

Definice 3. 5. 1. – Nechť máme neprázdnou množinu M a na ní definovanou binární operaci $\circ$, potom dvojici $(M, \circ)$ nazýváme *grupou*, jestliže

$\forall\, k, l, m \in M\!: (k \circ l) \circ m = k \circ (l \circ m)$, je asociativní,

$\exists e \in N\; \forall k \in M\!: e \circ k = k \circ e = k$, existuje neutrální prvek,

$\forall k \in N\; \exists k^{-1} \in M\!: k \circ k^{-1} = k^{-1} \circ k = e$, ke každému prvku existuje prvek inverzní.

Pokud je dále grupa, kde $\forall k, l \in M\!: k \circ l = l \circ k$, komutativní, hovoříme o *komutativní grupě*, nebo také *Abelově grupě*.

Příklady grup: $(Z, +), (Q, +)$. Za grupu nelze považovat $(Q, \;\cdot)$, jelikož neexistuje neutrální prvek k prvku 0.

Věta 7. – Mějme definovanou jakoukoliv grupu $(M, \circ)$ a prvek $c \in M$. Potom v této grupě nalezneme zrovna jeden neutrální prvek, a k prvku c najdeme zrovna jeden prvek $c^{-1} \in M$ k tomuto prvku inverzní.

Věta 8. – Mějme definovanou jakoukoliv grupu $M = (M, \circ)$, pak pro libovolné dva prvky $c, d \in M$ platí:

i) $(c \circ d)^{-1} = d^{-1} \circ c^{-1}$

ii) $(d^{-1})^{-1} = d$

Důkaz:

i) Z definice inverzního prvku víme, že složením základního prvku $(c \circ d) \in M$ a prvku k němu inverzního$(c \circ d)^{-1} \in M$, získáme neutrální prvek $e \in M$:

$$(c \circ d) \circ (c \circ d)^{-1} = c \circ [d \circ (c^{-1} \circ d^{-1})] = c \circ [(d \circ d^{-1}) \circ c^{-1}] =$$

$$c \circ (e \circ c^{-1}) = (c \circ c^{-1}) = e,$$

$$(c \circ d) \circ (d^{-1} \circ c^{-1}) = [(c \circ d) \circ d^{-1}] \circ c^{-1} = [c \circ (d \circ d^{-1})] \circ c^{-1} =$$

$$= (c \circ e) \circ c^{-1} = c \circ c^{-1} = e.$$

dále také platí

$$(d^{-1} \circ c^{-1}) \circ (c \circ d) = d^{-1} \circ [c^{-1} \circ (c \circ d)] = d^{-1} \circ [(c^{-1} c) \circ d] =$$

$$= d^{-1} \circ (e \circ d) = d^{-1} \circ d = e,$$

$$(c \circ d)^{-1} \circ (c \circ d) = [(c^{-1} \circ d^{-1}) \circ c] \circ d = [(c^{-1} \circ c) \circ d^{-1}] \circ d =$$

$$(e \circ d^{-1}) \circ d = d^{-1} \circ d = e.$$

Z toho dostáváme, že obě dvojice rovností se rovnají neutrálnímu prvku $e \in M$. Tudíž docházíme k rovnosti $(c \circ d)^{-1} = d^{-1} \circ c^{-1}$.

ii) Mějme prvek $d^{-1} \in M$ a k němu prvek $(d^{-1})^{-1}$, který budeme označovat inverzním prvkem. Z definice inverzního prvku opět dokážeme

$$(d^{-1})^{-1} \circ d^{-1} = d^{-1} \circ (d^{-1})^{-1} = e$$

a dále

$$d \circ d^{-1} = d^{-1} \circ d = e.$$

Tudíž opět docházíme k rovnosti, že obě strany rovnice se rovnají neutrálnímu prvku $e \in M$. Proto platí $(d^{-1})^{-1} = d$.

Věta 9. – Krácení lze provádět v každé grupě $M = (M, \circ)$.

Důkaz: Mějme grupu $M = (M, \circ)$, která obsahuje prvky $k, l, m \in M$. Pro prvek m existuje prvek m^{-1} inverzní.

Potom na každou rovnost $k \circ m = l \circ m$ pak můžeme aplikovat následující úpravy. Pro úpravu použijeme definice asociativnosti a existence neutrálního prvku.

$$k \circ m = l \circ m$$

$$\Downarrow \ \circ m^{-1}$$

$$(k \circ m) \circ m^{-1} = (l \circ m) \circ m^{-1}$$

$$\Downarrow \ asociativnost$$

$$k \circ (m \circ m^{-1}) = l \circ (m \circ m^{-1})$$

$$\Downarrow \ inverzní\ prvek$$

$$k \circ e = l \circ e$$

$$\Downarrow \ neutrální\ prvek$$

$$k = l.$$

Analogicky odvodíme rovnost $m \circ k = m \circ l$.

Věta 10. – Rovnice $k \circ x_1 = l$ a $x_2 \circ k = l$ mají v každé grupě $M = (M, \circ)$ zrovna jedno řešení $\forall k, l \in M$.

Důkaz: Nejprve odvodíme existenci obou řešení:

$$k \circ x_1 = l$$

$$\Downarrow \ k^{-1} \circ$$

$$k^{-1} \circ (k \circ x_1) = k^{-1} \circ l$$

$$\Downarrow \ asociativnost$$

$$(k^{-1} \circ k) \circ x_1 = k^{-1} \circ l$$

$$\Downarrow \ inverzní\ prvek$$

$$e \circ x_1 = k^{-1} \circ l$$

$$x_2 \circ k = l$$

$$\Downarrow \ \circ k^{-1}$$

$$(x_2 \circ k) \circ k^{-1} = l \circ k^{-1}$$

$$\Downarrow \ asociativnost$$

$$x_2 \circ (k \circ k^{-1}) = l \circ k^{-1}$$

$$\Downarrow \ inverzní\ prvek$$

$$x_2 \circ e = l \circ k^{-1}$$

$$x_1 = k^{-1} \circ l \qquad\qquad x_2 = l \circ k^{-1}$$

Tedy $$k \circ x_1 = k \circ (k^{-1} \circ l) = (k \circ k^{-1}) \circ l = e \circ l = l$$

$$x_2 \circ k = (l \circ k^{-1}) \circ k = l \circ (k^{-1} \circ k) = l \circ e = l.$$

Nyní předpokládejme, že musí existovat dvě řešení $x_{1a} \neq x_{1b}$.

$$x_{1a} \circ k = l, x_{1b} \circ k = l$$

$$\Downarrow$$

$$x_{1a} \circ k = x_{1b} \circ k$$

$$\Downarrow \circ k^{-1}$$

$$(x_{1a} \circ k) \circ k^{-1} = (x_{1b} \circ k) \circ k^{-1}$$

$$\Downarrow \textit{asociatovnost}$$

$$x_{1a} \circ (k \circ k^{-1}) = x_{1b} \circ (k \circ k^{-1})$$

$$\Downarrow \textit{inverzní prvek}$$

$$x_{1a} \circ e = x_{1b} \circ e$$

$$\Downarrow$$

$$x_{1a} = x_{1b}.$$

Kde $x_{1a} = x_{1b}$ znázorňuje spor.

Definice 3. 5. 2. – Mějme grupu $M = (M, \circ)$ a podgrupoid $L = (L, \circ)$ grupoidu M. Jestliže L je grupou, potom tento podgrupoid nazveme *podgrupou* grupy M.

Definice 3. 6. - Všechny 4 výše uvedené základní algebraické struktury $(X, \circ)$ nazýváme *konečné*, jestliže je konečná i množina X. Potom budeme udávat *řád* této množiny X, který je dán počtem všech jejích prvků.

Uveďme jednoduchý příklad na určení této výše uvedené algebraické struktury.

Příklad 11: Vyšetření algebraické struktury. Algebraickou strukturu reprezentuje množina

$$M = Z_S, \qquad k \blacksquare l = k + l, \forall k, l \in M,$$

kde Z_S je množina celých sudých čísel.

Řešení:

Nejdříve si určíme, zda je tato operace uzavřená na množině Z_S.

Ze součtu dvou sudých čísel dostaneme vždy za výsledek sudé číslo.

I. Vyšetření komutativnosti:

$$k \blacksquare l = l \blacksquare k$$
$$k + l = l + k$$

Operace je komutativní.

Můžeme tedy říct, že se jedná o grupoid. Budeme pokračovat ve vyšetřování dalších vlastností.

II. Vyšetření asociativnosti:

$$(k \blacksquare l) \blacksquare m = k \blacksquare (l \blacksquare m)$$
$$(k + l) + m = k + (l + m)$$

Operace je asociativní.

Jedná se tedy o pologrupu, jelikož operace je asociativní.

III. Vyšetření existence neutrálního prvku:

$$k \blacksquare e = e \blacksquare k = k$$

Vyšetříme existenci levého a pravého neutrálního prvku zvlášť:

$$P: \quad k + e = k \quad \Rightarrow \quad e = 0$$
$$L: \quad e + k = k \quad \Rightarrow \quad e = 0$$

Neutrální prvky levé a pravé strany se rovnají. Existuje tedy neutrální prvek $e = 0$.

Existuje neutrální prvek, tudíž se jedná o monoid.

IV. Vyšetření inverzního prvku:

$$k \blacksquare k^{-1} = k^{-1} \blacksquare k = e$$

Opět vyšetříme zvlášť levou a pravou stranu. Z předchozího kroku víme, že $e = 0$, proto do rovnice za e dosadíme 0.

$$P: \quad k + k^{-1} = 0$$
$$k^{-1} = -k$$
$$L: \quad k^{-1} + k = 0$$
$$k^{-1} = -k$$

Existuje inverzní prvek.

Jedná se tedy o grupu. Jelikož je i komutativní, můžeme říct, že jde o Abelovu grupa.

Nyní vypočtěme pár složitějších příkladů na algebraické struktury.

Příklad 12. Určete typ algebraické struktury $Z = (Z, \circ)$ na množině $Z = \{0,1,2,3,4\}$, kde je operace $\circ$ definována jako $x \circ y = x + 2y\ (modulo\ 5)$.

Řešení:

Pro vyřešení daného příkladu si sestavíme operační tabulku.

$\circ$	0	1	2	3	4
0	0	2	4	1	3
1	1	3	0	2	4
2	2	4	1	3	0
3	3	0	2	4	1
4	4	1	3	0	2

Tato operace je neomezeně definovaná v Z. Můžeme prozatím dojít k závěru, že se jedná o grupoid. Nyní se pokusíme vyšetřit asociativnost. Asociativnost ověříme uvedením vhodného protipříkladu. Zjišťujeme, že pro (2,2,3)

$$(x \circ y) \circ z = (x + 2y) \circ z = (2 \circ 2) \circ 3 = 1 \circ 3 = 2$$

$$x \circ (y \circ z) = x \circ (x + 2y) = 2 \circ (2 \circ 3) = 2 \circ 3 = 3$$

$L \neq P$, operace není asociativní.

Ještě vyšetříme, zda se nejedná o komutativní grupoid. Zvolíme si $(2,3)$

$$x \circ y = 2 \circ 3 = 3$$

$$y \circ x = 3 \circ 2 = 2$$

$L \neq P$, nejedná se o komutativní operaci. Můžeme tedy konstatovat, že algebraická struktura definovaná na Z je grupoidem.

Příklad 13: Určete jaký typ algebraické struktury je binární operace průnik na množině $M = \{\emptyset, \{3\}, \{6\}, \{12\}, \{3,6\}, \{3,12\}, \{6,12\}, \{3,6,12\}\}$.

Řešení:

Pro jednoduší vyřešení zadaného příkladu si sestrojíme operační tabulku, ve které vyznačíme průnik daných prvků.

$\cap$	$\emptyset$	$\{3\}$	$\{6\}$	$\{12\}$	$\{3,6\}$	$\{3,12\}$	$\{6,12\}$	$\{3,6,12\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{3\}$	$\emptyset$	$\{3\}$	$\emptyset$	$\emptyset$	$\{3\}$	$\{3\}$	$\emptyset$	$\{3\}$
$\{6\}$	$\emptyset$	$\emptyset$	$\{6\}$	$\emptyset$	$\{6\}$	$\emptyset$	$\{6\}$	$\{6\}$
$\{12\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{12\}$	$\emptyset$	$\{12\}$	$\{12\}$	$\{12\}$
$\{3,6\}$	$\emptyset$	$\{3\}$	$\{6\}$	$\emptyset$	$\{3,6\}$	$\{3\}$	$\{6\}$	$\{3,6\}$
$\{3,12\}$	$\emptyset$	$\{3\}$	$\emptyset$	$\{12\}$	$\{3\}$	$\{3,12\}$	$\{12\}$	$\{3,12\}$
$\{6,12\}$	$\emptyset$	$\emptyset$	$\{6\}$	$\{12\}$	$\{6\}$	$\{12\}$	$\{6,12\}$	$\{6,12\}$
$\{3,6,12\}$	$\emptyset$	$\{3\}$	$\{6\}$	$\{12\}$	$\{3,6\}$	$\{3,12\}$	$\{6,12\}$	$\{3,6,12\}$

Tato operace je neomezeně definována na množině M. Můžeme říci, že se jedná o grupoid.

Jelikož se prvky v záhlaví tabulky rovnají prvkům na diagonále. Můžeme operaci průnik na množině označit jako komutativní.

U průniku víme, že je vždy asociativní. Jelikož je operace průniku asociativní, jedná se o strukturu zvanou pologrupa.

Existuje řádek i sloupec shodný se záhlavím tabulky, tudíž existuje na množině i neutrální prvek a je jím $e = \{3,6,12\}$. Operace je i monoidem.

Pro existenci inverzního prvku musí existovat k danému prvku vždy prvek opačný. Neutrálním prvkem je v tomto případě množina $e = \{3,6,12\}$ a nedokážeme najít žádnou dvojici prvků, které v průniku dají právě neutrální prvek. V tabulce bychom jako k sobě vzájemně inverzní prvky označili ty, jejichž výsledkem je $\{3,6,12\}$, takové tam však kromě neutrálního prvku samotného nejsou.

Docházíme k závěru, že $(M,\cap)$ je komutativním monoidem.

4. Zobrazení algebraických struktur s jednou binární operací. Homomorfismus a Izomorfismus

Nyní se budeme zabývat zobrazením, zachovávající algebraické operace, které v algebře označujeme jako homomorfismus.

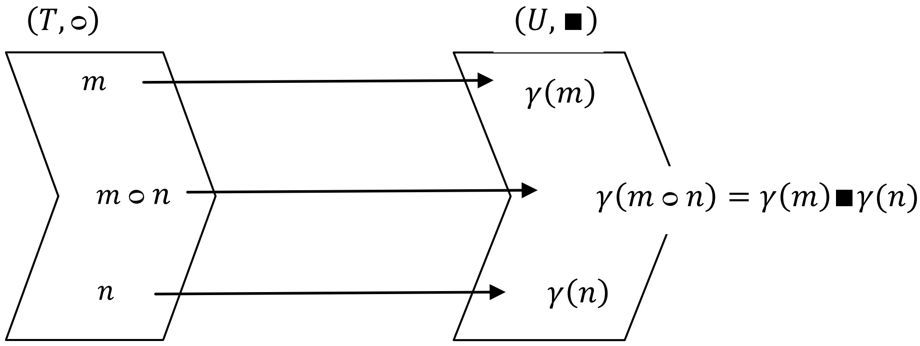
Definice 4. 1. - Mějme algebraické struktury s jednou binární operací

$$T = (T, \circ), U = (U, \blacksquare).$$

Zobrazení $\gamma: T \to U$, pro které

$$\forall m, n \in T: \gamma(m \circ n) = \gamma(m) \blacksquare \gamma(n)$$

prohlásíme homomorfním zobrazením (homomorfismem) algebraických struktur.



Věta 11. - Mějme pologrupy $T = (T, \circ), U = (U, \blacksquare)$ a homomorfní zobrazení $\gamma: T \to U$. Vycházíme z toho, že nezáleží na pořadí, zda nejdříve provedeme operaci $\circ$ a pak ji zobrazíme, nebo prvně prvky pologrup zobrazíme a potom provedeme operaci $\blacksquare$.

$$\begin{array}{ccc} (m, n) & \overrightarrow{\circ} & m \circ n \\ \downarrow \gamma & & \downarrow \gamma \\ \gamma(m), \gamma(n) & \overrightarrow{\blacksquare} & \gamma(m) \blacksquare \gamma(n). \end{array}$$

Věta 12. - Mějme monoidy $T = (T, \circ), U = (U, \blacksquare)$ a homomorfní zobrazení $\gamma: T \to U$. Pokud monoid $T = (T, \circ)$ má neutrální prvek e, pak obsahuje i monoid $U = (U, \blacksquare)$ neutrální prvek e_1

$$\gamma(e) = e_1.$$

Důkaz: Mějme jakýkoliv prvek monoidu $u \in U$. Potom se musí vyskytovat vždy alespoň jeden prvek $m \in T$, aby platilo $\gamma(m) = u$. Pokud tedy $\gamma(e) = e_1$, a $e \in T$ se rovná neutrálnímu prvku grupoidu T, potom

$$u = \gamma(m) = \gamma(m \circ e) = \gamma(m) \blacksquare \gamma(e) == u \blacksquare e_1$$

$$u = \gamma(m) = \gamma(e \circ m) = \gamma(e) \blacksquare \gamma(m) = e_1 \blacksquare u.$$

Prvek e_1 je tedy neutrálním prvkem monoidu $U = (U, \blacksquare)$.

Věta 13. – Mějme grupy $T = (T, \circ), U = (U, \blacksquare)$ s neutrálními prvky e a e_1, a homomorfní zobrazení $\gamma: T \to U$. Pokud grupa $T = (T, \circ)$ pro $a \in T$ má inverzní prvek a^{-1}, potom i grupa $U = (U, \blacksquare)$ pro $\gamma(a)$ má inverzní prvek $\left(\gamma(a)\right)^{-1}$

$$\gamma(a^{-1}) = \left(\gamma(a)\right)^{-1}$$

Důkaz: Pro inverzní prvky v grupě $T = (T, \circ)$ platí

$$a \circ a^{-1} = a^{-1} \circ a = e$$

tedy

$$\gamma(a \circ a^{-1}) = \gamma(a) \blacksquare \gamma(a^{-1}) = \gamma(e) = e_1.$$

$$\gamma(a^{-1} \circ a) = \gamma(a^{-1}) \blacksquare \gamma(a) = \gamma(e) = e_1.$$

a to znamená, že prvek $\gamma(a^{-1})$ je inverzním prvkem k prvku $\gamma(a)$ v grupě $U = (U, \blacksquare)$.

Věta 14. - Pokud se jedná o surjektivní zobrazení $\gamma: T \to U$, považujeme $U = (U, \blacksquare)$ za homomorfní obraz $T = (T, \circ)$, a píšeme

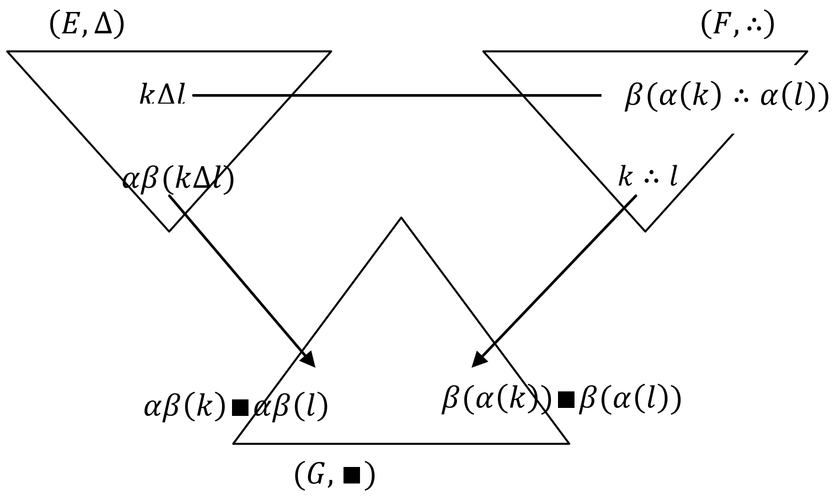
$$(T, \circ) \sim (U, \blacksquare).$$

Věta 15. - Mějme Abelův grupoid (pologrupu, monoid, grupu). Jejich homomorfním obrazem je opět Abelův grupoid (…).

Důkaz: Mějme $T = (T, \circ)$ Abelův grupoid (pologrupu, monoid, grupu) a homomorfní zobrazení $\gamma: T \to U$ na grupoid (…) $U = (U, \blacksquare)$. Potom existují vždy dva prvky $u, v \in U$ a dva prvky $m, n \in T$, pro které $\gamma(m) = u, \gamma(n) = v$

$$u \blacksquare v = \gamma(m) \blacksquare \gamma(n) = \gamma(m \circ n) = \gamma(n \circ m) = \gamma(n) \blacksquare \gamma(m) = v \blacksquare u.$$

Věta 16. – Mějme grupoidy (pologrupy, monoidy, grupy) $E = (E, \Delta), F = (F, \therefore), G = (G, \blacksquare)$ a homomorfní zobrazení $\alpha: E \to F \quad \beta: F \to G$. Potom jako homomorfismus grupoidů (…) E do G označujeme složené zobrazení $\alpha\beta$.



Důkaz: Mějme $k, l \in E$, potom pro homomorfismy α a β platí

$$\alpha \cdot \beta(k \, \Delta \, l) = \beta\big(\alpha(k \, \Delta \, l)\big) = \beta\big(\alpha(k) \therefore \alpha(l)\big) = \beta\big(\alpha(k)\big)\blacksquare\beta\big(\alpha(l)\big) = \alpha \cdot \beta(k)\blacksquare\alpha \cdot \beta(l)$$

a z toho docházíme, že $\alpha \cdot \beta$ je homomorfismem E do G.

Definice 4. 2. – Mějme grupoidy (pologrupy, monoidy, grupy) $T = (T, \circ), U = (U, \blacksquare)$. Pokud je jejich zobrazení $\gamma: T \to U$ bijektivní, nazýváme toto zobrazení izomorfní. Hovoříme tedy o izomorfním zobrazení (izomorfismu) $\gamma: T \to U$. A značíme

$$(T, \circ) \cong (U, \blacksquare)$$

Každé izomorfní zobrazení má samozřejmě všechny vlastnosti, které jsme uvedli u homomorfního zobrazení.

Stručný přehled základních vlastností izomorfismu:

Věta 17. – Mějme izomorfní grupoidy (pologrupy, monoidy, grupy) $(T, \circ) \cong (U, \blacksquare)$ a izomorfní zobrazení $\gamma: T \to U$.

I. Je-li grupoid $T = (T, \circ)$ pologrupou, potom je pologrupou i grupoid $U = (U, \blacksquare)$,
II. je-li pologrupa $T = (T, \circ)$ monoidem s neutrálním prvkem, potom je monoidem s neutrálním prvkem i pologrupa $U = (U, \blacksquare)$,

III. je-li monoid $T = (T, \circ)$ grupou s inverzními prvky, potom je grupou s inverzními prvky i monoid $U = (U, \blacksquare)$,

IV. Grupoid (pologrupa, monoid, grupa) $T = (T, \circ)$ jsou Abelovou, potom i grupoid (pologrupa, monoid, grupa) $U = (U, \blacksquare)$ jsou Abelovou.

Příklad 14: Rozhodněte, zda zobrazení $f: A \to B$ je homomorfismem grupy $(A, °)$ do grupy $(B, \blacksquare)$ je-li:

$$(A, °) = (Z, +);\ (B, \blacksquare) = (R, +);\ \varphi(z) = 2x + 1, \forall x \in Z.$$

Řešení:

$$\forall x, y \in Z: \varphi(x \circ y) = \varphi(x) \blacksquare \varphi(y)$$

$$\varphi(x + y) = 2(x + y) + 1 = 2x + 2y + 1$$

$$\varphi(x) + \varphi(y) = 2x + 1 + 2y + 1 = 2x + 2y + 2$$

$$x \neq y \Longrightarrow \varphi(x) \neq \varphi(y)$$

Vzhledem k tomu, že neplatí $\varphi(x \circ y) = \varphi(x) \blacksquare \varphi(y)$, resp. $\varphi(x + y) = \varphi(x) + \varphi(y)$, nejedná se o homomorfismum.

5. ALGEBRAICKÉ STRUKTURY SE DVĚMA BINÁRNÍMI OPERACEMI

Definice 5. 1. – Mějme neprázdnou množinu K, na které je definována alespoň jedna binární operace. Potom hovoříme o algebraických strukturách s binárními operacemi. Množinu K můžeme označit také jako nosič algebraické struktury.

Je-li definována $(K, +, *)$ hovoříme o algebraické struktuře se dvěma binárními operacemi.

Výčet algebraických struktur se dvěma binárními operacemi:

Polookruh, okruh, obor integrity, těleso, komutativní polookruh (okruh, obor integrity, těleso).

Než začneme definovat jednotlivé struktury se dvěma algebraickými strukturami, zavedeme si několik nových pojmů. O sčítání $(E, +)$ budeme hovořit jako o aditivní operaci, o násobení $(E, \cdot)$ budeme hovořit jako o multiplikativní operaci. Neutrální prvek z $(E, +)$ budeme nazývat prvkem nulovým a z $(E, \cdot)$ prvkem jednotkovým. Prvek inverzní v operaci $(E, +)$ budeme označovat prvek opačný a v operaci $(E, \cdot)$ prvek převrácený. Ještě si nadefinujeme pojem distributivní, kde

$$\forall e, f, g \in E: (e + f) \cdot g = e \cdot g + f \cdot g \quad \wedge \quad g \cdot (f + e) = g \cdot f + g \cdot e.$$

Definice 5. 2. – Mějme algebraickou strukturu $E = (E, +, \cdot)$.

Pokud $(E, +)$ je Abelova pologrupa $\forall\, e, f \in E: e + f = f + e$

$\forall\, e, f, g \in E: (e + f) + g = e + (f + g)$

a $(E, \cdot)$ je pologrupa $\forall\, e, f, g \in E: (e \cdot f) \cdot g = e \cdot (f \cdot g)$

a operace $(E, \cdot)$ je distributivní vůči $(E, +)$, potom hovoříme o *polookruhu*.

Definice 5. 3. 1. – Polookruh $E = (E, +, \cdot)$ pojmenujeme

I. komutativní (Abelův), pokud je komutativní i multiplikativní grupoid $(E, \cdot)$
II. polookruh s nulovým prvkem, pokud $(E, +)$ je aditivní monoid
III. polookruh s jednotkovým prvkem, pokud $(E, \cdot)$ je multiplikativní monoid

Příklad polookruhů: $(N, +, \cdot)$.

Definice 5. 3. 2. – O algebraické struktuře $F = (F, +, \cdot)$ hovoříme jako o *okruhu*, pokud je $(F, +)$ Abelova grupa $\forall\, e, f \in F: e + f = f + e$

$\forall\, e, f, g \in F: (e + f) + g = e + (f + g)$

$\exists 0 \in F, \forall e \in F: e + 0 = 0 + e = e$

$\forall e \in F, \exists(-e) \in F: e + (-e) = (-e) + e = 0,$

$(F, \cdot)$ je pologrupou $\forall\, e, f \in F: e \cdot f = f \cdot e$

$\forall\, e, f, g \in F: (e \cdot f) \cdot g = e \cdot (f \cdot g)$

a operace $(F, \cdot)$ je distributivní vůči $(F, +)$.

Věta 18. – Okruh $F = (F, +, \cdot)$ nazveme

I. komutativní (Abelův), pokud je komutativní i multiplikativní pologrupa $(F, \cdot)$
II. polookruh s jednotkovým prvkem, pokud $(F, \cdot)$ je multiplikativní monoid

Příklady okruhů: $(Z, +, \cdot)$, $(Q, +, \cdot)$.

Definice 5. 3. 3. – Pokud v okruhu $F = (F, +, \cdot)$ existují prvky $f \neq 0, g \neq 0$, potom pro $f \cdot g = 0$, jsou prvky f, g dělitelé nuly.

Definice 5. 4. – O algebraické struktuře $G = (G, +, \cdot)$ hovoříme jako o *oboru integrity*, pokud $(G, +, \cdot)$ je komutativním okruhem, ve kterém se nevyskytují dělitelé nuly a operace $(G, \cdot)$ je distributivní vůči $(G, +)$.

Příklady oboru integrity: $(Z, +, \cdot), (Q, +, \cdot)$.

Definice 5. 5. – O algebraické struktuře $H = (H, +, \cdot)$ hovoříme jako o *tělesu*, pokud existuje okruh H a nenulové prvky $(H - \{0\}, \cdot)$ tvoří grupu. Je-li grupa nenulových prvků komutativní, hovoříme o komutativním (Abelově) tělesu.

ZÁVĚR

Ve své bakalářské práci jsem se snažila objasnit teorii algebraických struktur s jednou binární operací. Seznámit čtenáře se základními definicemi a větami, potřebnými k pochopení tohoto tématu.

Postupně jsme probrali grupoidy, pologrupy, monoidy a grupy, a ke každé z těchto struktur jsme uvedli jednoduché příklady, které vedou ke snazšímu pochopení těchto struktur. K pochopení tohoto tématu nám taky velice pomohlo objasnění základních binárních operací potřebných ke zjišťování typu algebraické struktury.

Se studiem algebraických struktur, také souvisí jejich zobrazení, tedy homomorfismus a izomorfismus. V úplném závěru jsme se ještě zmínili o existenci algebraických struktur se dvěma binárními operacemi. Studiem těchto struktur, jsme se však již více nezabývali.

Seznam použité literatury a zdrojů

[1] EMANOVSKÝ, Petr. *Algebraické struktury ve vysokoškolské přípravě učitelů matematiky*. Olomouc: Univerzita Palackého, 2000. 112 s. ISBN 80-244-0066-9.

[2] LIBICHER, Jaroslav. *Algebra I. Algebraické struktury*. Ostrava: Pedagogická fakulta v Ostravě, 1973. 125 s.

[3] NOVOTNÁ, Vilma. *Binární operace a algebraické struktury*. Ostrava: Ostravská univerzita v Ostravě, Pedagogická fakulta, 2006. 101 s. Dostupné z WWW: https://stag1.osu.cz/web_doc/1191412596186.pdf.

[4] TESKOVÁ, Libuše. *Algebraické struktury*. 43 s. Dostupné z WWW: http://home.zcu.cz/~teskova/WWW-KMA/ALG.pdf.

[5] DRÁBEK, J., HORA, J. *Algebra. Polynomy a rovnice*. Plzeň: Západočeská univerzita v Plzni, 2001. 125 s. ISBN 80-7082-787-4.

[6] LEGÉŇ, Antonín. *Grupy, okruhy, sväzy*. Bratislava: Alfa, vydavatelstvo technickej a ekonomickej literatúry, 1980. 280 s.

[7] KUROŠ, Gennadievič, Alexandr. *Kapitoly z obecné algebry*. Vyd. 2. Přeložil J. Blažek, L. Koubek. Praha: Československá akademie věd Academia, 1977. 312 s.

[8] BORŮVKA, Otakar. *Úvod do teorie grup*. Praha, Přírodovědné vydavatelství, 1952. 156 s.

[9] EMANOVSKÝ, Petr. *Cvičení z algebry. Algebraické struktury*. Olomouc: Univerzita Palackého, 1993. 31 s. ISBN 80-7067-296-X.

[10] KOPTA, Jan. *Algebraické struktury.* Ústí nad Labem: Pedagogická fakulta, 1985. 120 s.

[11] KOPECKÝ, Milan. Základy algebry. Olomouc: Univerzita Palackého, 1998. 129 s. ISBN 80-7067-891-7.

[12] EMANOVSKÝ, Petr. Algebra 4. Olomouc: Univerzita Palackého, 2004. 82 s. ISBN 80-244-0799-X.

RESUMÉ

This bachelor thesis deals with the study of algebraic structures with one binary operation, and their display. For determining the types of algebraic structures helps us to clarify the binary operations. Then we can say that grupoid is structure with unlimited defined binary operations. Semigroup is grupoid, which is also associative. Monoid is a semigroup with neutral element. Group is a monoid with the inverse element. Moreover, if for all these structures valid that they are commutative, they are called Abel. These structures determine their display, homomorphism and isomorphism.