ZÁKLADNÍ POJMY VÝROKOVÉ LOGIKY

Výrok je každé sdělení, o němž má smysl říci, že je buď pravdivé nebo nepravdivé.

Pozn. Není důležité, zda o pravdivosti či nepravdivosti výroku umíme rozhodnout. Podstatné je, zda má smysl o pravdivosti uvažovat, zda má smysl položit si otázku: „Je pravda, že...?“

Rozhodněte, které z následujících vět jsou výroky:

1. Právě začalo pršet.
2. Na Marsu existují živé organismy.
3. Karel IV. byl v Praze r. 1348.
4. Rozvoj matematických představ.
5. Pojď k tabuli.
6. Číslo 4 je dělitelem čísla 134.
7. 100 : 5 = 20
8. 4 + x = 9

Ve výrokové logice nás nezajímá konkrétní obsah výroků, ale jejich pravdivost (pravdivostní hodnota).

Každému výroku je možné přiřadit pravdivostní hodnotu:

Je-li výrok pravdivý, je jeho pravdivostní hodnota 1.

Je-li výrok nepravdivý, jeho pravdivostní hodnota je 0.

Negace výroku *A* je výrok $\neg A$, který je pravdivý v případě, že výrok *A* je nepravdivý.

Složené výroky

Z jednoduchých výroků můžeme tvořit složené výroky pomocí tzv. výrokotvorných spojek:

- „a“, „a současně“, „a zároveň“ ($\wedge$)
- „nebo“ ($\vee$)
- „buď, nebo“ ($\veebar$)
- „jestliže, pak“; „*A* implikuje *B*“ ($\Rightarrow$)
- „právě tehdy, když“ ($\Leftrightarrow$)

Konjunkce výroků *A, B* je výrok $A \wedge B$, který je pravdivý v případě, že jsou oba výroky pravdivé.

Disjunkce (alternativa) výroků *A, B* je výrok $A \vee B$, který je pravdivý v případě, že je alespoň jeden z výroků *A, B* pravdivý.

Ostrá disjunkce výroků *A, B* je výrok $A \veebar B$, který je pravdivý v případě, že je právě jeden z výroků *A, B* pravdivý.

Implikace výroků *A, B* je výrok $A \Rightarrow B$, který je **ne**pravdivý jen v případě, že první výrok je pravdivý a druhý výrok je nepravdivý. Ve všech ostatních případech je implikace pravdivá.

Ekvivalence výroků *A, B* je výrok $A \Leftrightarrow B$, který je pravdivý v případě, že oba výroky mají stejnou pravdivostní hodnotu.

Pomocí výrokotvorných spojek můžeme výroky různě skládat a uvažovat pak o jejich pravdivosti (obsah jednotlivých výroků nás nezajímá):

Mluvíme pak o **výrokových formulích.** Jsou to zápisy, ve kterých se objevují výrokové proměnné *A,B, P, Q*, .. log. spojky, závorky a to tak, že když dosadíme za výrokové proměnné konkrétní výroky, dostaneme výrok: Např. $\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$.

Pak nás zajímá, jaké pravdivostní hodnoty nabývá výsledný výrok v závislosti na pravdivosti výroků *A, B*.

Typy formulí: tautologie, kontradikce, splnitelná výr. formule.

Tautologie výrokové logiky – příklady.

Základní množinové pojmy, vztahy mezi množinami, množinové operace

Množina je takový souhrn objektů, že o každém objektu můžeme rozhodnout, zda do uvažovaného souhrnu objektů patří nebo nepatří.

Pro každou množinu A a pro každý objekt *a* nastane právě jedna ze dvou možností:

buď $a \in A$ nebo $a \notin A$.

Množina může být určena výčtem prvků nebo pomocí charakteristické vlastnosti, tj. jako obor pravdivosti výrokové formy.

Např. $A = \{2, 3, 5, 7\} = \{x \in N; x \text{ je prvočíslo} \wedge x < 10\}$

Množina A je podmnožinou (částí) množiny B, právě tehdy, když každý prvek množiny A je též prvkem množiny B. Zapisujeme $\mathbf{A \subset B}$.

Množina A se rovná množině B (značíme **A = B**) právě tehdy, když každý prvek množiny A je prvkem množiny B a současně každý prvek množiny B je prvkem množiny A.

(Platí tedy: A = B, právě když $A \subset B$ a $B \subset A$.)

Doplněk množiny A vzhledem k základní množině Z je množina všech prvků množiny Z, které nepatří do množiny A.

$A' = \{x \in Z; x \notin A\}$

Sjednocení množin A, B je množina prvků, které patří alespoň do jedné z množin A, B.

$A \cup B = \{x \in Z; x \in A \vee x \in B\}$

Průnik množin A, B je množina prvků, které patří do množiny A a současně do množiny B.

$A \cap B = \{x \in Z; x \in A \wedge \in B\}$

Rozdíl množin A, B je množina, která obsahuje právě ty prvky množiny A, které nepatří do množiny B

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

Symetrický rozdíl množin A, B je množina, která obsahuje ty prvky, které patří právě do jedné z množin.

$A \Delta B = \{x \in Z; x \in A \underline{\vee} x \in B\}$

Množinové situace lze přehledně graficky znázornit pomocí množinových (tzv. Vennových) diagramů. Množiny jsou v nich znázorněny pomocí oblastí roviny ohraničených jednoduchými uzavřenými křivkami. V případě dvou (tří, čtyř, *n*) množin je základní množina rozdělena na 4 (8, 16, 2^n) elementárních polí.

Vlastnosti množinových operací a jejich ověřování.

Kvantifikované výroky. Výrokové formy. Logické úlohy.

Ve školské matematice, ale i běžně v různých životních situacích se používají vyjádření typu

všichni, ne všichni, někdo, nikdo, žádný, každý, kterýkoliv, některý, aspoň jeden apod., která vedle číslovek také vyjadřují počet nebo množství – jsou to tzv. kvantifikátory (v širším smyslu).

V logice vystačíme se dvěma **kvantifikátory:**

Obecný kvantifikátor (∀x – „pro každé x platí …“)

Existenční kvantifikátor (∃x – „existuje aspoň jedno x …, pro které platí …“)

Negace kvantifikovaných výroků.

Není pravda, že všichni jsou tady. -- Aspoň jeden tady není.

Není pravda, že si všichni umyli ruce. – Aspoň jeden si neumyl ruce.

Není pravda, že někdo neumí zpívat. -- Každý umí zpívat.

Není pravda, že někdo tady umí hrát na kytaru. – Nikdo (každý) tady neumí hrát na kytaru.

Výrokové formy.

Sdělení, v nichž se vyskytuje jedna nebo více proměnných. V případě, že za proměnné dosadíme z tzv. definičního oboru výrokové formy, dostaneme z ní výrok.

Obvykle nás zajímá **obor pravdivosti** výrokové formy, tj. množina prvků, pro něž dostaneme z výrokové formy pravdivý výrok.

Příklady:

Žák X dnes chybí.

$x + 10 < 13$

(Obor pravdivosti závisí na tom, jak je určen definiční obor)

Z výrokové formy můžeme také dostat výrok, vážeme-li všechny proměnné pomocí kvantifikátorů: obecného∀nebo existenčního ∃.

Např. ∀x ∈ N: x + 10 < 13 (Pro každé přirozené číslo x je ...) je nepravdivý výrok

∃ x ∈ N: x + 10 < 13 (Existuje přirozené číslo x takové, že ...) je pravdivý výrok.

Pravidla odvozování

Úsudek – spojení několika výroků, kdy poslední z nich (závěr) se odvozuje z předcházejících (tzv. premis)

Pravidla odvozování – formálně správné úsudky.

Např.

$$\frac{\neg X, X \vee Y}{Y}$$

$$\frac{X \Rightarrow Y, X}{Y}$$

$$\frac{X \Rightarrow Y, \neg Y}{\neg X}$$

Pravidla odvozování používáme při odvozování důsledků z daných předpokladů. Za výrokové proměnné dosazujeme výroky (jednotlivé, složené nebo kvantifikované).

O správnosti těchto úsudku se můžeme přesvědčit pomocí tabulek pravdivostních hodnot příslušných formulí (musí jít o tautologie)

Pozor na NESPRÁVNÝ úsudek, který se často užívá místo (x): $\frac{X \Rightarrow Y, \neg X}{\neg Y}$

Přesvědčte se o jeho nesprávnosti, tj. ohodnoťte výrokovou formuli:

$$[(X \Rightarrow Y) \wedge \neg X] \Rightarrow \neg Y$$

Pravidla odvozování predikátové logiky

Podobně, jako se vytvářejí pravidla odvozování výrokové logiky, lze tvořit pravidla odvozování predikátové logiky, tzn., že se v jejich zápisech vyskytují kvantifikované výroky obsahující výrokové formy o několika proměnných.

Na ukázku uvedeme jeden jednoduchý případ. Ověříme, že následující zápis je zápisem pravidla odvozování:

$$\frac{(\forall x \in D)[A(x) \Rightarrow B(x)], (\exists x \in D)[A(x)]}{(\exists x \in D)[B(x)]}.$$

Připomeňme, že vedení úvah o pravidlech odvozování predikátové logiky je rozsáhlé a značně komplikované (zejména uvažujeme-li výrokové formy o více proměnných). Závěry o těchto pravidlech se však většinou opírají o již připomenutá pravidla odvozování výrokové logiky (větší rozsáhlost možností je dána možnou volbou kvantifikátorů.

Příklady

1. Kdo se dobře učil, stal se váženým člověkem. Nejsem vážený člověk, tedy jsem se dobře neučil. (P)

2. Kdo se dobře učil, stal se váženým člověkem. Jsem vážený člověk, tedy jsem se dobře učil. (N)

3. Žádný student není bohatý člověk a někteří moudří lidé nejsou bohatí. Odtud plyne, že někteří studenti jsou moudří lidé. (N)

4. Každý student je moudrý člověk a někteří studenti jsou bohatí. Odtud plyne, že někteří moudří lidé jsou bohatí. (P)

5. Každý levný výrobek je dobře prodejný a některé levné výrobky jsou kvalitní. Odtud plyne, že některé dobře prodejné výrobky jsou kvalitní. (P)

6. Každý duševně zdravý člověk může studovat logiku, přičemž žádný z Karlových přátel ji studovat nemůže. Potom žádný z Karlových přátel není duševně zdráv. (P)

Binární relace v množině, vlastnosti binárních relací, ekvivalence, uspořádání.

Binární relace v množině M je libovolná podmnožina kartézského součinu M x M.

Znázornění binárních relací

Kartézský graf relace R – sestrojíme dvě na sebe kolmé přímky x, y (vodorovnou a svislou). Na vodorovnou přímku (osu) znázorníme pomocí bodů všechny prvky množiny, z níž vybíráme první složky dvojic, na svislou přímku (osu) znázorníme pomocí bodů všechny prvky množiny, z níž vybíráme druhé složky dvojic. (Obvykle jsou sousední body na obou osách od sebe stejně vzdáleny.) Uspořádanou dvojici $[a,b]\in R$ znázorníme bodem, který je průsečíkem dvou přímek procházejících body a, b a rovnoběžných po řadě se svislou a vodorovnou osou.

Uzlový graf relace R v množině M - v rovině znázorníme pomocí bodů (tzv. uzlů) všechny prvky množiny M (pokud bychom znázorňovali relaci z množiny A do množiny B, pak znázorníme všechny prvky sjednocení množina A a B). Uspořádanou dvojici $[a,b]\in R$ znázorníme pomocí šipky (tzv. orientované hrany), která vychází z uzlu a a směřuje do uzlu b. V případě, že $a = b$, nazýváme šipku smyčkou. Pokud sou v relaci R dvojice $[a,b]$ a [b,a], znázorníme je "dvojšipkou" (tzv. neorientovanou hranou).

Vlastnosti relací v množině M

Binární relace R v množině M je **reflexivní** právě tehdy, když

$(\forall x\in M)$ $([x,x]\in R)$, tzn. obsahuje všechny uspořádané dvojice [x,x], kde $x\in M$.

Binární relace R v množině M je **antireflexivní** právě tehdy, když

$(\forall x\in M)$ $([x,x]\notin R)$, tzn. neobsahuje žádnou uspořádanou dvojici typu [x,x], kde $x\in M$.

Binární relace R v množině M je **symetrická** právě tehdy, když

$$(\forall x,y\in M)\ ([x,y]\in R \Rightarrow [y,x]\in R),$$

tzn. s každou uspořádanou dvojicí [x,y] obsahuje i dvojici ([y,x].

Binární relace R v množině M je **antisymetrická**, právě tehdy, když

$$(\forall x,y\in M)\ ((x \neq y \wedge [x,y]\in R) \Rightarrow [y,x]\notin R),$$

tzn. s žádnou dvojicí [x,y] různých prvků neobsahuje dvojici [y,x].

Binární relace R v množině M je **tranzitivní** právě tehdy, když

$$(\forall x,y,z\in M)\ ([x,y]\in R \wedge [y,z]\in R) \Rightarrow [x,z]\in R),$$

tzn. jestliže se v relaci vyskytují „na sebe navazující dvojice“, pak musí relace obsahovat i dvojici, jejíž první složkou je 1. složka z první dvojice a druhou složkou je 2. složka z druhé dvojice.

Binární relace R v množině M je **souvislá** právě tehdy, když

$$(\forall x,y\in M)\ (x \neq y \Rightarrow ([x,y]\in R \vee [y,x]\in R),$$

tzn. každé dva různé prvky z množiny M musí být „spolu v relaci“.

Binární relaci U v množině M nazýváme **ostré lineární uspořádání** v M, právě když je antisymetrická, tranzitivní, souvislá a antireflexivní.

Pro každou ostře lineárně uspořádanou množinu platí, že **každý** její prvek má **jednoznačně stanovené** pořadí.

První a poslední prvek ostře lineárně uspořádané množiny.

Uspořádaná množina je dobře uspořádaná, jestliže každá její neprázdná podmnožina má první prvek. Každá konečná ostře lineárně uspořádaná množina je dobře uspořádaná.

Binární relaci R v množině M nazýváme **relací ekvivalence** na M**,** právě když je reflexivní, symetrická a tranzitivní.

Každá relace ekvivalence na množině M vytváří **rozklad** této množiny, což je systém neprázdných podmnožin (tzv. tříd rozkladu) množiny M takových, že průnik každých dvou tříd je prázdná množina a sjednocení všech tříd rozkladu tvoří množinu M.

Jinak lze také říci, že říci, že **rozklad** množiny M je systém neprázdných podmnožin (tzv. tříd rozkladu) množiny M takových, že každý prvek množiny M patří právě do jedné z těchto tříd.

Zobrazení z množiny do množiny, typy zobrazení

Nechť **R** je relace z množiny A do množiny B splňující vlastnosti: Ke každému prvku $a \in A$ existuje nejvýše jeden prvek $b \in B$ takový, že $[a,b] \in \mathbf{R}$. Tato relace se nazývá **zobrazení z množiny A do množiny B.** Značíme R: $A \rightarrow B$.

Nechť **R** je zobrazení z množiny A do množiny B.

- Jestliže $[a,b] \in \mathbf{R}$, pak prvek $a \in A$ nazýváme **vzorem** prvku $b \in B$ v zobrazení **R**; prvek $b \in B$ nazýváme **obrazem** prvku $a \in A$ v zobrazení **R**.
- Množina $O_1(\mathbf{R}) = \{a \in A$: existuje $b \in B$ takové, že $[a,b] \in \mathbf{R}\}$ se nazývá **definiční obor** zobrazení **R**. Platí $O_1(\mathbf{R}) \subset A$.
- Množina $O_2(\mathbf{R}) = \{b \in B$: existuje $a \in A$ takové, že $[a,b] \in \mathbf{R}\}$ se nazývá **obor hodnot** zobrazení **R**. Platí $O_2(\mathbf{R}) \subset B$.

Příklad . Jsou dány množiny A = {x, y, z}, B = {a, b}. Rozhodněte, zda dané relace z množiny A do množiny B jsou zobrazení z A do B, případně určete definiční obor a obor hodnot zobrazení.

a) $\mathbf{R_1}$ = {[x,a], [y,b], [z,a], [z,b]},
b) $\mathbf{R_2}$ = {[x,a], [z,b]},
c) $\mathbf{R_3}$ = {[x,a], [y,a], [z,a]}.

Rozlišujeme následující **typy zobrazení R**:

I) Je–li $O_1(\mathbf{R}) = A \wedge O_2(\mathbf{R}) \subset B \wedge O_2(\mathbf{R}) \neq B$, nazývá se **R <u>zobrazení množiny A do množiny B</u>**.

II) Je–li $O_1(\mathbf{R}) \subset A \wedge O_1(\mathbf{R}) \neq A \wedge O_2(\mathbf{R}) = B$, nazývá se **R <u>zobrazení z množiny A na množinu B</u>**.

III) Je–li $O_1(\mathbf{R}) = A \wedge O_2(\mathbf{R}) = B$, nazývá se **R <u>zobrazení množiny A na množinu B</u>**.

IV) Je–li $O_1(\mathbf{R}) \subset A \wedge O_1(\mathbf{R}) \neq A \wedge O_2(\mathbf{R}) \subset B \wedge O_2(\mathbf{R}) \neq B$, nazývá se **R <u>zobrazení z množiny A do množiny B</u>**.

Příklad . Jsou dány množiny A = {x, y, a, c}, B = {c, x, b, z}.

a) Rozhodněte, o jaký typ zadaných zobrazení se jedná?

1) **R** = {[x,z], [c,c], [y,c]}.

2) **S** = {[x,z], [y,z], [a,z], [c,x]}.

b) Zapište výčtem prvků jednu binární relaci z množiny A do množiny B, která není zobrazením.

c) Zapište výčtem prvků

1) jedno zobrazení $\mathbf{R_1}$ typu z množiny A do množiny B,

2) jedno zobrazení $\mathbf{R_2}$ množiny A do množiny B,

3) jedno zobrazení množiny A na množinu B,

4) jedno zobrazení z množiny A na množinu B.

Zobrazení **R** z množiny A do množiny B se nazývá **prosté** právě tehdy, když relace $\mathbf{R^{-1}}$ je zobrazení z množiny B do množiny A.

Důsledek: Zobrazení **R** z množiny A do množiny B je **prosté** právě tehdy, když

a) ke každému $y \in B$ existuje nejvýše jedno $x \in A$ takové, že $[x,y] \in \mathbf{R}$,

b) ke každým dvěma různým vzorům $x_1, x_2 \in A$ přiřadíme dva různé obrazy $y_1, y_2 \in B$ v zobrazení **R.**

Hovoříme pak o:

- Prostém zobrazení množiny A do množiny B,
- Prostém zobrazení z množiny A na množinu B,
- Prostém zobrazení množiny A na množiny B,
- Prostém zobrazení z množiny A do množiny B.

Prosté zobrazení množiny A na množinu B nazýváme **bijektivní zobrazení** nebo také **vzájemně jednoznačné zobrazení**.

Příklad . Jsou dány množiny A = {1, 2, 3, 4}, B = {a, b, c, d}. Rozhodněte, o jaký typ zobrazení se jedná a zda je toto zobrazení prosté:

a) $\mathbf{R_1}$ = {[1,a], [2,c], [3,d]},

b) $\mathbf{R_2}$ = {[1,a], [2,c], [3,d], [4,a]},

c) $\mathbf{R_3}$ = {[2,a], [1,c], [3,b], [4,d]}.

Permutací konečné množiny A nazýváme každé prosté zobrazení množiny A na množinu A (vzájemně jednoznačné zobrazení).

Příklad . Zapište všechny permutace tříprvkové množiny A = {x, y, z}.

Definice: Nechť **R** je zobrazení z množiny M do množiny N a **S** je zobrazení z množiny N do množiny K. Pak relace **R** ∘ **S** je zobrazení a nazývá se **složené zobrazení** ze zobrazení **R** a **S**.

Příklad . Složte permutace $\mathbf{P_2} \circ \mathbf{P_3}$, $\mathbf{P_3} \circ \mathbf{P_2}$, $\mathbf{P_4} \circ \mathbf{P_6}$ z předchozího příkladu..

Řekneme, že množiny A, B jsou **ekvivalentní** právě tehdy, když existuje prosté zobrazení množiny A na množinu B. Značíme A ~ B.

Příklad : Dány množiny A = {a, b, c}, B = {x, y}, C = {1, 2, 3}. Rozhodněte, které množiny jsou ekvivalentní.

Ř: Množiny A, B nejsou ekvivalentní (neexistuje prosté zobrazení množiny A na množinu B). Množiny A, C jsou ekvivalentní (existuje prosté zobrazení množiny A na množinu C, například R = {[a,3],[b,1],[c,2]}), tj. **A ~ C**.

Množina M je **vlastní podmnožinou** množiny N právě tehdy, když M je podmnožinou N a současně $M \neq N$.

Řekneme, že množina A je **konečná** právě tehdy, když žádná vlastní podmnožina množiny A není ekvivalentní s množinou A.

Řekneme, že množina B je **nekonečná** právě tehdy, když existuje alespoň jedna vlastní podmnožina množiny B, která je ekvivalentní s množinou B.

Příklad: Uvažujme množinu $\mathbb{N}$ všech přirozených čísel a množinu S všech kladných sudých čísel. Zjistěte, zda jsou ekvivalentní.

Řešení: Připomeneme, že $\mathbb{N}$ = {1, 2, 3, 4, 5,…}, S = {2, 4, 6, 8 , 10,…}.
Uvažujme relaci $R = \{[x,y] \in \mathbb{N} \times S;\ y = 2x\}$.

Relace R je prosté zobrazení množiny $\mathbb{N}$ na množinu S, neboť
ke každému $x \in \mathbb{N}$ existuje právě jedno $y \in S$ takové, že $[x,y] \in R$,
ke každému $y \in S$ existuje právě jedno $x \in \mathbb{N}$ takové, že $[x,y] \in R$.
Tedy $\mathbb{N} \sim S$.

Množina $\mathbb{N}$ všech přirozených čísel je nekonečná, neboť je ekvivalentní s množinou S všech kladných sudých čísel, přičemž S je vlastní podmnožinou množiny $\mathbb{N}$.

Nechť A, B jsou **konečné** množiny. Pak platí: $A \sim B \Leftrightarrow |A| = |B|$, tedy dvě konečné množiny jsou ekvivalentní, právě když mají stejný počet prvků.

Binární operace v množině

Definice 1: Nechť M je libovolná neprázdná množina. **Binární operací** $\circ$ v množině M rozumíme zobrazení z množiny kartézského součinu M x M do množiny M.

- Jestliže v binární operaci je vzoru $[x,y] \in M \times M$ přiřazen obraz $z \in M$, píšeme:
  1. $x \circ y = z$; prvek $z \in M$ se nazývá **výsledek operace** $\circ$.
  2. $\circ: M \times M \to M$.

Poznámka 1. Zápisu $[[x,y], z] \in \circ$, odpovídá zápis $x \circ y = z$ (tj. z je výsledek operace $\circ$).

Příklad 1. a) Zápisu $[[1,2], 3] \in +$, odpovídá $1 + 2 = 3$ (tj. 3 je výsledek operace sčítání čísel 1 a 2).

binární operace sčítání **součet**

b) Zápisu $[[2,3], 6] \in \cdot$, odpovídá $2 \cdot 3 = 6$ (tj. 6 je výsledek operace násobení čísel 2 a 3).

binární operace násobení **součin**

Poznámka 2. Označení binárních operací: +, ·, $\circ$, $*$, $\square$,..

Příklady binárních operací ve školské matematice:

1) Sčítání (+), odčítání (-), násobení (·), dělení (**:**), umocňování,… (pracujeme s nimi v číselných množinách).
2) Sjednocení ($\cup$), průnik ($\cap$), rozdíl (-), symetrický rozdíl (Δ) množin,… (pracujeme s nimi v systémech množin).

Určení binární operace: Tabulkou nebo předpisem.

Vlastnosti binárních operací:

Definice : Binární operace $\circ$ v množině M, která má vlastnost, že je definována pro každou uspořádanou dvojici $[x,y] \in M \times M$, se nazývá operace **neomezeně definovaná** v množině M (zkráceně operace **definovaná na** množině M). Značíme **ND**.

Symbolicky: $(\forall x, y \in M)(\exists z \in M)[x \circ y = z]$.

Definice: Binární operace $\circ$ definovaná na množině M (je ND), se nazývá **komutativní** právě tehdy, když platí:

$$(\forall x, y \in M)[x \circ y = y \circ x].$$

Značíme **K**.

Definice: Binární operace $\circ$ definovaná na množině M, se nazývá **asociativní** právě tehdy, když platí:

$$(\forall x, y, z \in M)[(x \circ y) \circ z = x \circ (y \circ z)].$$

Značíme **A**.

Definice: Nechť v množině M je definována binární operace $\circ$. Existuje-li prvek $e \in M$, pro který platí:

$$(\forall x \in M)[x \circ e = e \circ x = x].$$

Pak se prvek $e \in M$ nazývá **neutrálním prvkem** množiny M vzhledem k operaci $\circ$.

Značíme **EN**.

Poznámka. Je-li operace $\circ$ komutativní, pak v zápisu vlastnosti **EN** lze vynechat jedna ze dvou stran rovnosti $x \circ e$ nebo $e \circ x$.

Definice : Nechť v množině M je definována binární operace $\circ$ a nechť e je neutrální prvek množiny M vzhledem k operaci $\circ$. Prvek $\bar{a} \in M$ nazýváme **inverzním prvkem** k prvku $a \in M$ v operaci $\circ$ v množině M právě tehdy, když platí:

$$\bar{a} \circ a = a \circ \bar{a} = e.$$

Jestliže $(\forall a \in M)(\exists \bar{a} \in M)[\bar{a} \circ a = a \circ \bar{a} = e]$, řekneme, že ke každému prvku množiny M existuje prvek inverzní vzhledem k operaci $\circ$. Značíme **EI**.

Poznámka . Je-li operace $\circ$ komutativní, pak v zápisu vlastnosti **EI** lze vynechat jedna ze dvou stran rovnosti $\bar{a} \circ a = a \circ \bar{a}$.

Definice : Říkáme, že binární operace $\circ$ definovaná na množině M má vlastnost **řešitelnost základních rovnic** právě tehdy, když platí:

$$(\forall a, b \in M)\ )(\exists x, y \in M)[\ a \circ x = b \quad y \circ a = b].$$

Značíme **ZR**.

Poznámka. Je-li operace ○ komutativní, pak v zápisu vlastnosti **ZR** lze vynechat jedna z výrokových forem $a \circ x = b$ nebo $y \circ a = b$.

Definice: Nechť v množině M je definována binární operace ○. Existuje-li prvek $g \in M$, pro který platí:

$$(\forall x \in M)[\ x \circ g = g \circ x = g].$$

Pak se prvek g nazývá **agresivním** prvkem množiny M vzhledem k operaci ○.

Určování vlastností operací

I. **Určených předpisem** – přímým výpočtem

II. **Určených tabulkou**:

ND – tabulka zcela vyplněna prvky množiny M

K – tabulka souměrná podle hlavní diagonály

A – kromě výjimek nelze z tabulky přímo poznat – viz dále

EN – existuje řádek a sloupec shodný se záhlavím tabulky

EI – v každém řádku a každém sloupci tabulky je neutrální prvek

ZR – v každém řádku i sloupci tabulky jsou všechny prvky množiny M

Agresivní prvek $g \in M$ poznáme tak, že v celém jemu příslušejícím řádku i sloupci se vyskytuje pouze prvek g.

Užitečné vztahy: $K \Rightarrow ND$, $A \Rightarrow ND$, $EI \Rightarrow EN$ (užívají se v obměněném tvaru)

$$A \Rightarrow (EI \Leftrightarrow ZR)$$

Určování asociativnosti z tabulek:

1. Pohledem (velmi zřídka)

2. Ověřením všech možných trojic prvků (s využitím cvičení 9 – 13, s. 123 – 124) (těžkopádné a zdlouhavé)

3. Využitím obměny implikace $A \Rightarrow ND$ a implikace $A \Rightarrow (EI \Leftrightarrow ZR)$

4. Podle tvrzení: „ Operace, která splňuje EN $\wedge$ EI $\wedge$ ZR a současně není asociativní, existuje na množině o nejméně pěti prvcích“.

Užití na příkladech:

ad 1. Např.

o	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

ad 3. Nejčastější případ – rozbor implikace A $\Rightarrow$ (EI $\Leftrightarrow$ ZR). Je-li u EI a ZR rozdílná pravdivostní hodnota, pak operace není asociativní. Jsou-li u EI a ZR pravdivostní hodnoty 1, pak postupujeme podle bodu 4 (v písemných pracích jsou zadávány tabulky o maximálně čtyřech prvcích). Jsou-li u EI a ZR pravdivostní hodnoty 0, pak je nutno postupovat podle bodu 1 nebo 2. Zpravidla jde o bod 1, kdy určíme asociativnost přímo z tabulky.

Algebraické struktury s jednou operací

Uspořádaná dvojice (M, $\circ$), kde M je neprázdná množina, ve které je definována binární operace $\circ$, se nazývá **algebraická struktura s jednou operací.**

Příklad : Příklad algebraických struktur: ($\mathbb{N}$, +), ($\mathbb{C}$, -), ($\mathbb{Q}$ - {0}, :), ($\mathbb{R}$, $\cdot$)

Definice:

I. Algebraická struktura (M, $\circ$) se nazývá **grupoid** právě tehdy, když operace $\circ$ je neomezeně definovaná v množině M (ND).
II. Grupoid (M, $\circ$), jehož operace $\circ$ je asociativní, se nazývá **pologrupa** (ND, A).
III. Pologrupa (M, $\circ$) taková, že v M existuje neutrální prvek vzhledem k operaci (M, $\circ$) a ke každému prvku $a \in$ M existuje prvek inverzní $\bar{a} \in$ M, se nazývá **grupa** (ND, A, EN, EI).

Jestliže v případech I., II., III. je operace $\circ$ komutativní, pak hovoříme o komutativním grupoidu, komutativní pologrupě, komutativní grupě.

	Vlastnost operace ○	Algebraická struktura
(M, ○)	ND	Grupoid
	ND K	Komutativní grupoid
	ND A	Pologrupa
	ND A K	Komutativní pologrupa
	ND A EN EI	Grupa
	ND A EN EI K	Komutativní grupa

Příklady algebraických struktur s jednou operací

1. $(\mathbb{N}, +)$ … komutativní pologrupa s neutrálním prvkem $e = 0$
2. $(\mathbb{N}, -)$ … není ani grupoid
4. $(\mathbb{N}, \cdot)$ … komutativní pologrupa s neutrálním prvkem $e = 1$
5. $(\mathbb{N}, :)$ …není ani grupoid
6. $(\mathbb{C}, +)$ … komutativní grupa
7. $(\mathbb{C}, -)$ … grupoid s vlastností ZR

operace odčítání není K*:* $a - x = b$ $y - a = b$, $x = a - b$ $y = b + a$,
$a - b \in \mathbb{C}$ $b + a \in \mathbb{C}$, tj. obě rovnice jsou pro lib. $a, b \in \mathbb{C}$ vždy řešitelné

8. $(\mathbb{C}, \cdot)$ … komutativní pologrupa
9. $(\mathbb{C}, :)$ …není ani grupoid
10. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ … komutativní grupy s neutrálním prvkem
11. $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$… grupoid s vlasností ZR
12. $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$… komutativní pologrupy
13. $(\mathbb{Q}, :)$, $(\mathbb{R}, :)$… není ani grupoid
14. $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$ … komutativní grupa

Důkazy v komutativní grupě:

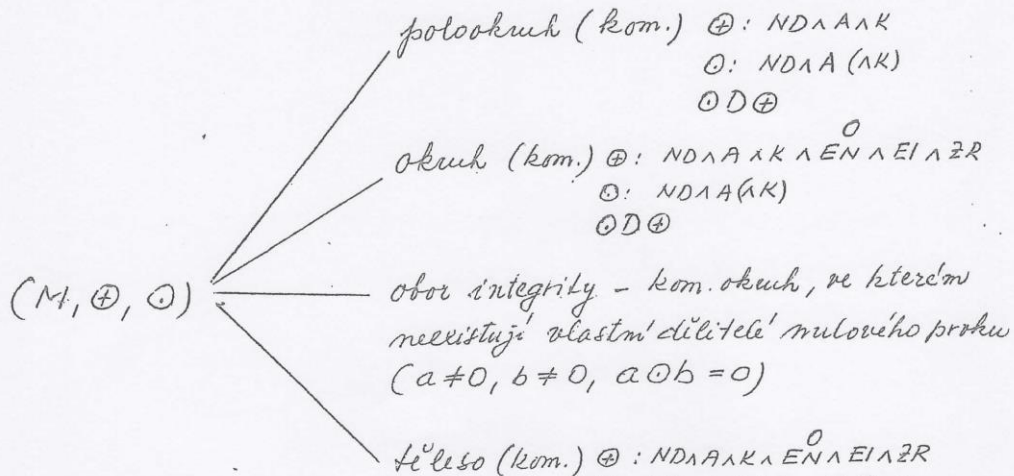
$\overline{a \cdot b} = \bar{a} \cdot \bar{b}$, $\quad \bar{\bar{a}} = a$, $\quad a \cdot c = b \cdot c \Rightarrow a = b$ apod.

Algebraická struktury se dvěma operacemi

$(M, \oplus, \odot)$

$\oplus$ - sčítám, EN - nulový prvek, 0; $\bar{a} = -a$ opačný prvek k prvku a

$\odot$ - násobím, EN - jednotkový prvek, 1; $\bar{a} = \bar{a}^{-1} = \frac{1}{a}$ převrácený prvek k a



Př. $(N, +, \cdot)$ - komutat. pologrupa s oběma neutrálními prvky, který není okruhem

$(\mathbb{C}, +, \cdot)$ - obor integrity, není tělesem

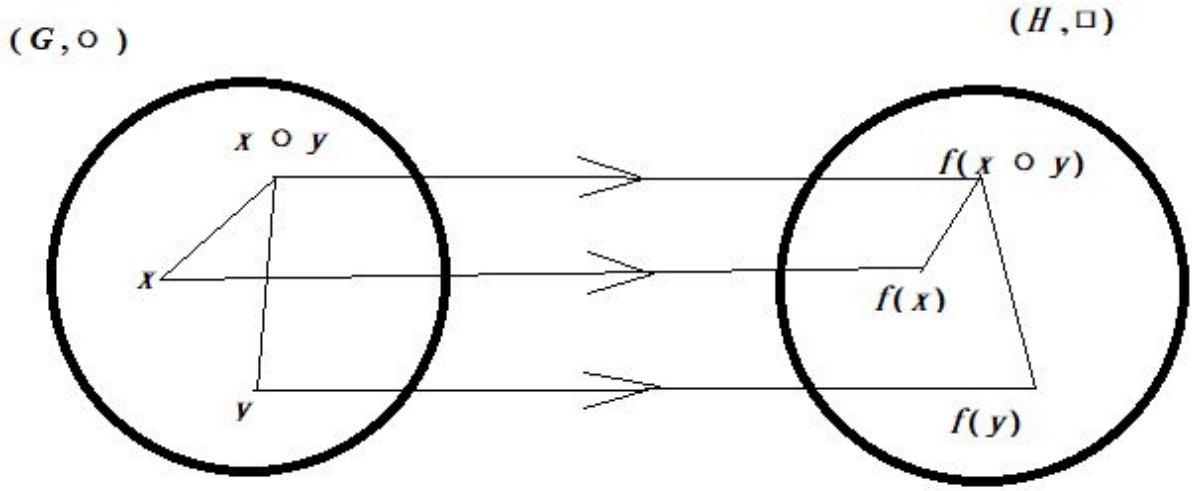
$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ - tělesa, obory integrity

$(M, \oplus, \odot)$ - pologrupa; Ex.-li prvek x takový, že $a = b \oplus x = x \oplus b$, pak x se nazývá rozdíl prvků a, b. $x = a \ominus b$

Ex.-li prvek x takový, že $a = b \odot x = x \odot b$, pak x se nazývá podíl prvků a, b. $x = a \oslash b$

~~Okruh $(M, \oplus, \odot)$ $x = a \ominus b$ def. $x = a \ominus b = a \oplus (-b)$~~

Těleso $(M, \oplus, \odot)$ $x = a \oslash b$ def. $x = a \oslash b = a \odot \frac{1}{b}$, $b \neq 0$



Nechť f je vzájemně jednoznačné zobrazení množiny G na množinu H, nechť $(G, \circ)$, $(H, \square)$ jsou alg. struktury (alespoň grupoidy). Pak zobrazení f nazveme **izomorfismus** $(G, \circ)$ na $(H, \square)$, jestliže platí:

$$(\forall\, x, y \in G)\; f(x \circ y) = f(x) \square f(y).$$

Píšeme $(G, \circ) \cong (H, \square)$.

Nechť $(G, \circ)$, $(H, \square)$ jsou struktury (alespoň grupoidy), nechť $(G, \circ) \cong (H, \square)$ (tj. obě struktury jsou izomorfní). Pak platí:

1. $G \sim H$.

2. Má-li jedna z operací $\circ$, $\square$ některou z vlastností K, A, EN, EI, ZR, má tuto vlastnost i druhá z těchto operací.
Obě operace mají tedy tytéž vlastnosti.

3. Obě algebraické struktury $(G, \circ)$, $(H, \square)$ jsou téhož typu.

Příklad: Nechť $G = \{a, b, c, d\}$, $H = \{1, -1, i, -i\}$.

o	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

·	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

Množina H je množina všech řešení rovnice $x^4 = 1$ v oboru komplexních čísel, operace · na množině H je pak „obyčejné“ násobení. Kdo není seznámen s komplexními čísly, tomu postačí vědět, že $i \cdot i = -1$.

Definujeme-li nyní vzájemně jednoznačné zobrazení f množiny G na množinu H předpisem $f(a) = 1, f(b) = -1, f(c) = i, f(d) = -i$, snadno se přesvědčíme pohledem na tabulky, že toto zobrazení je izomorfismus, tedy platí vztah $(G, \circ) \cong (H, \cdot)$.