

Logické systémy

doc. RNDr. Jana Galanová, PhD.

RNDr. Peter Kaprálik, PhD.

Mgr. Marcel Polakovič, PhD.

KAPITOLA 1

Úvodné pojmy

V tejto časti uvádzame základné pojmy, prevažne z diskkrétnej matematiky, ktoré sú potrebné pre štúdium logických systémov. V prvom rade sa dohodnime na tomto označení číselných množín:

$$\mathbf{N} = \{0, 1, 2, \dots, n, \dots\},$$

$$\mathbf{N}^+ = \{1, 2, \dots, n, \dots\},$$

$\mathbf{Z}$ – množina všetkých celých čísel,

$\mathbf{R}$ – množina všetkých reálnych čísel,

$\mathbf{R}^+$ – množina všetkých kladných reálnych čísel.

1. Zobrazenia a operácie

DEFINÍCIA 1.1. Nech A, B sú množiny. Pravidlo (predpis) f , ktoré každému prvku $x \in A$ priradí jeden prvok $y \in B$, sa nazýva **zobrazenie množiny A do množiny B** a označuje sa $f : A \rightarrow B$. Prvok y priradený prvku x nazývame **obrazom prvku x** a píšeme $y = f(x)$ (tiež $x \mapsto y$). Prvok x nazývame **vzorom prvku y** . Množina A sa nazýva **obor** (tiež **definičný obor**) a množina B **koobor zobrazenia f** .

PRÍKLAD 1.1. Nech $A = \{a, b, c\}, B = \{0, 1\}$. Potom $f : A \rightarrow B; a \mapsto 1, b \mapsto 0, c \mapsto 1$ je zobrazenie množiny A do množiny B , lebo každý prvok množiny A má len jeden obraz. ■

DEFINÍCIA 1.2. Zobrazenie $f : A \rightarrow B$ sa nazýva

injektívne (tiež **prosté**), ak pre každé $x_1, x_2 \in A$, platí: ak $x_1 \neq x_2$, potom $f(x_1) \neq f(x_2)$;

surjektívne, ak každý prvok $y \in B$ má vzor (t.j. ku každému $y \in B$ existuje také $x \in A$, že $y = f(x)$);

bijektívne, ak je injektívne aj surjektívne.

PRÍKLAD 1.2. Zobrazenie f z predchádzajúceho príkladu nie je injektívne, lebo $a \neq c$, ale $f(a) = 1 = f(c)$. Je však surjektívne, lebo každý prvok množiny B má vzor, konkrétne vzorom prvku 0 je b a vzorom prvku 1 je a . ■

DEFINÍCIA 1.3. **Karteziánskym súčinom množín** $M_1, M_2, \dots, M_n$ nazývame množinu

$$M_1 \times M_2 \times \dots \times M_n = \{(x_1, x_2, \dots, x_n); x_1 \in M_1, x_2 \in M_2, \dots, x_n \in M_n\}.$$

V prípade, že $M_1 = M_2 = \dots = M_n = M$, namiesto $M \times M \times \dots \times M$ píšeme M^n .

Prvok $(x_1, x_2, \dots, x_n)$ sa nazýva **usporiadaná n -tica**.

Usporiadané n -tice $(x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n)$ sú rovnaké práve vtedy, keď $x_1 = y_1, x_2 = y_2, \dots, x_n = y_n$.

PRÍKLAD 1.3. Karteziánskym súčinom množín $A = \{a, b, c\}, B = \{0, 1\}$ je množina $A \times B = \{(a, 0), (a, 1), (b, 0), (b, 1), (c, 0), (c, 1)\}$. ■

DEFINÍCIA 1.4. Nech A je množina, n je prirodzené číslo. Každé zobrazenie $h : A^n \rightarrow A$ nazývame **n -árnou operáciou na množine A** . Špeciálne pre $n = 1$ sa operácia h nazýva **unárna** a pre $n = 2$ **binárna**.

PRÍKLAD 1.4. Funkcia $f(x, y) = x + y$ je binárna operácia na množine $\mathbf{R}$, pretože je definovaná pre každé $x, y \in \mathbf{R}$ a tiež $f(x, y) \in \mathbf{R}$.

Funkcia $g(x, y) = x \cdot y$ je tiež binárnou operáciou na $\mathbf{R}$, pretože jej definičný obor je $\mathbf{R} \times \mathbf{R}$ a pre každé $x, y \in \mathbf{R}$ platí $g(x, y) \in \mathbf{R}$.

Funkcia $h(x, y) = x - y$ nie je binárna operácia na $\mathbf{R}^+$, pretože rozdiel každých dvoch kladných reálnych čísel nemusí byť kladné reálne číslo, napr. $2 - 3 = -1 \notin \mathbf{R}^+$, pričom $2, 3 \in \mathbf{R}^+$.

Funkcia $k(x) = x + 3$ je unárna operácia na $\mathbf{R}$, pretože pre každé $x \in \mathbf{R}$ platí $x + 3 \in \mathbf{R}$. ■

POZNÁMKA 1.1. Nech $\square : A^2 \rightarrow A$ je binárna operácia na množine A . Potom obraz dvojice $(a, b) \in A^2$ namiesto $\square(a, b)$ často označujeme symbolom $a \square b$.

DEFINÍCIA 1.5. Binárna operácia $\square : A^2 \rightarrow A$ sa nazýva

komutatívna, ak pre každé $a, b \in A$ platí $a \square b = b \square a$,

asociatívna, ak pre každé $a, b, c \in A$ platí $(a \square b) \square c = a \square (b \square c)$.

Prvok $e \in A$ sa nazýva **neutrálny prvok** binárnej operácie $\square$ na množine A , ak pre všetky $x \in A$ platí $x \square e = e \square x = x$.

POZNÁMKA 1.2. Binárnu operáciu, ktorú označujeme $\cdot$, obvykle nazývame **súčin** a jej neutrálny prvok (pokiaľ existuje) nazývame **jednotkový prvok**.

Binárnu operáciu, ktorú označujeme $+$, obvykle nazývame **súčet** a jej neutrálny prvok (pokiaľ existuje) nazývame **nulový prvok**.

PRÍKLAD 1.5. Binárna operácia $\circ : \mathbf{R}^2 \rightarrow \mathbf{R}, x \circ y = x^3 y^3$ je komutatívna, lebo pre všetky $x, y \in \mathbf{R}$

$$x \circ y = x^3 y^3 = y^3 x^3 = y \circ x,$$

ale nie je asociatívna, lebo napr. pre $x = \sqrt[3]{2}, y = 1, z = \sqrt[9]{2}$

$$(x \circ y) \circ z = (\sqrt[3]{2} \circ 1) \circ \sqrt[9]{2} = (2 \cdot 1) \circ \sqrt[9]{2} = 8 \sqrt[3]{2}$$

$$x \circ (y \circ z) = \sqrt[3]{2} \circ (1 \circ \sqrt[9]{2}) = \sqrt[3]{2} \circ (1 \cdot \sqrt[3]{2}) = 2 \cdot 2 = 4$$

Pre neutrálny prvok $e \in \mathbf{R}$ by malo platiť $x \circ e = x$, teda $x^3 e^3 = x$ a po úprave (za predpokladu, že $x \neq 0$) $e = \sqrt[3]{x^{-2}}$. Prvok e musí byť pre všetky x rovnaký, čo v našom prípade nenastáva. To znamená, že táto operácia nemá neutrálny prvok. ■

DEFINÍCIA 1.6. Nech $\square, \triangle$ sú binárne operácie na množine A . Hovoríme, že **binárna operácia $\square$ je distributívna vzhľadom k binárnej operácii $\triangle$** , ak pre všetky $x, y, z \in A$

$$\begin{aligned} x \square (y \triangle z) &= (x \square y) \triangle (x \square z), \\ (y \triangle z) \square x &= (y \square x) \triangle (z \square x). \end{aligned}$$

PRÍKLAD 1.6. Na množine $\mathbf{N}^+$ uvažujme binárne operácie:

$+$: $(\mathbf{N}^+)^2 \rightarrow \mathbf{N}^+$ – štandardné sčítanie,

$\square$: $(\mathbf{N}^+)^2 \rightarrow \mathbf{N}^+, x \square y = x$,

$$\triangle : (\mathbf{N}^+)^2 \rightarrow \mathbf{N}^+, x \triangle y = y.$$

Binárna operácia $\square$ je distributívna vzhľadom k operácii $\triangle$, lebo pre všetky $x, y, z \in \mathbf{N}^+$

$$\begin{aligned} x \square (y \triangle z) &= x \square z = x, \\ (x \square y) \triangle (x \square z) &= x \triangle x = x = x \square (y \triangle z), \\ (y \triangle z) \square x &= z \square x = z, \\ (y \square x) \triangle (z \square x) &= y \triangle z = z = (y \triangle z) \square x. \end{aligned}$$

Analogicky sa dá ukázať, že operácia $\triangle$ je distributívna vzhľadom k operácii $\square$. Naproti tomu operácie $\square, \triangle$ nie sú distributívne vzhľadom k operácii $+$, čo vyplýva z faktu

$$\begin{aligned} 1 \square (2 + 3) &= 1 \square 5 = 1, \\ (1 \square 2) + (1 \square 3) &= 1 + 1 = 2 \neq 1 \square (2 + 3), \\ (2 + 3) \triangle 1 &= 5 \triangle 1 = 1 \\ (2 \triangle 1) + (3 \triangle 1) &= 1 + 1 = 2 \neq (2 + 3) \triangle 1. \end{aligned}$$

■

2. Jazyk nad abecedou

Jedným z prostriedkov výmeny informácií medzi ľuďmi je ľudská reč. Jej významové jednotky sú vety. Vety sa skladajú zo slov a slová z písmen. V tejto časti zovšeobecníme tieto pojmy z prirodzených jazykov.

DEFINÍCIA 1.7. Neprázdnu množinu X nazývame **abecedou**. Prvky množiny X nazývame **písmenami** (abecedy X). Konečnú postupnosť písmen abecedy X nazývame **slovom** nad X . Počet písmen v slove w nad abecedou X nazývame **dĺžkou slova** w a označujeme ju $|w|$. Množinu všetkých slov nad abecedou X označujeme X^+ .

Nech $\nabla \notin X^+$. Symbol ∇ nazývame **prázdny slovo** nad X a priradujeme mu dĺžku nula. Množinu všetkých slov nad abecedou X spolu s prázdny slovom označujeme X^* .

PRÍKLAD 1.7. Nech $X = \{a, b, c, d, e\}$. X je abeceda, jej písmenami sú a, b, c, d, e . Slová sú napr. $aa, baba, cda, e, dedaecb$. Slovo aa má dĺžku 2, slovo $baba$ má dĺžku 4 ($|baba| = 4$), $|cda| = 3$, $|e| = 1$, $|dedaecb| = 8$. ■

PRÍKLAD 1.8. Nech $X = \{0, 1\}$. Napíšeme postupne všetky slová nad X dĺžok 1, 2, 3. *Riešenie.*

Dĺžku 1 majú dve slová: 0, 1.

Dĺžku 2 majú štyri slová: 00, 01, 10, 11.

Dĺžku 3 má osem slov: 000, 001, 010, 100, 110, 101, 011, 111. ■

Poznamenajme, že všetkých slov s dĺžkou n nad dvojprvkovou abecedou je 2^n .

DEFINÍCIA 1.8. Binárnu operáciu $\bullet$ na množine X^* definovanú:

$$\begin{aligned} x_1 x_2 \dots x_n \bullet y_1 y_2 \dots y_m &= x_1 x_2 \dots x_n y_1 y_2 \dots y_m \\ x_1 x_2 \dots x_n \bullet \nabla &= \nabla \bullet x_1 x_2 \dots x_n = x_1 x_2 \dots x_n \\ \nabla \bullet \nabla &= \nabla \end{aligned}$$

kde $x_1 x_2 \dots x_n \in X^+, y_1 y_2 \dots y_m \in X^+$ a ∇ je prázdne slovo, nazývame **zreťazením slov** z X^* . Množinu X^+ spolu s binárnou operáciou $\bullet$ zreťazenia nazývame **voľná pologrupa nad množinou X** (množina X^* spolu s operáciou zreťazenia slov sa nazýva **voľná pologrupa s jednotkou** alebo tiež **monoid**). Každú podmnožinu množiny X^* nazývame **jazykom** nad abecedou X .

Poznamenajme, že tak ako pri násobení reálnych čísel namiesto $x.y$ píšeme xy , tak aj pre binárnu operáciu $\bullet$ namiesto $x \bullet y$ píšeme xy . Potom môžeme definíciu zreťazenia slov z X^* prepísať takto:

$$\begin{aligned}(x_1x_2 \dots x_n)(y_1y_2 \dots y_m) &= x_1x_2 \dots x_ny_1y_2 \dots y_m \\ x_1x_2 \dots x_n \nabla &= \nabla x_1x_2 \dots x_n = x_1x_2 \dots x_n \\ \nabla \nabla &= \nabla\end{aligned}$$

PRÍKLAD 1.9. Slovo 01100 nad abecedou $X = \{0, 1\}$ je zreťazením slov 0 a 1100, tiež zreťazením slov 01 a 100, ale nie je zreťazením slov 000 a 11. ■

PRÍKLAD 1.10. Ak $X = \{0, 1\}$, tak zreťazením slov 1101, ∇ je slovo 1101 ∇ = 1101. Slovo 1101 je zreťazením slov 11, 01, ako aj zreťazením slov 1, ∇ , 101, pretože $(1\nabla)101$ = 1101. ■

VETA 1.1. Pre binárnu operáciu zreťazenia slov na množine X^* platí asociatívny zákon

$$(xy)z = x(yz).$$

Dôkaz. Ak $x, y, z \in X^*$, tak podľa definície zreťazenia pre slová xy, z, x, yz platí $(xy)z = xyz, x(yz) = xyz$, teda $(xy)z = x(yz)$. □

Tak, ako je obvyklé v prípade platnosti asociatívneho zákona, budeme označovať $xyz = (xy)z = x(yz)$.

PRÍKLAD 1.11. Nech $X = \{0, 1, 2\}$. Potom zreťazením slov 01, 210, ∇ , 22 je slovo 01(210(∇ 22)) = 01(21022) = 0121022. Slovo 120021 je zreťazením slov 12, 00, ∇ , 21, ale aj zreťazením slov 12 ∇ , $\nabla\nabla$, 0021. ■

3. Výroková logika

3.1. Výroky.

Mnohé vety, ktoré používame v prirodzených jazykoch (slovenčina, angličtina, atď.) alebo v jazykoch vedných odborov sú pravdivé, mnohé sú nepravdivé (i keď o ich pravdivosti či nepravdivosti nemusíme vedieť práve rozhodnúť) a sú vety, o pravdivosti ktorých nemá zmysel vôbec uvažovať (napr. „Neotravujte ma s matematikou!“). V tejto časti sa budeme zaoberať vetami, o pravdivosti ktorých má zmysel uvažovať.

DEFINÍCIA 1.9. Vety, ktoré sú pravdivé a vety, ktoré sú nepravdivé, majú **pravdivostnú hodnotu**. Vety, ktoré majú pravdivostnú hodnotu a tá sa nemení, sa nazývajú **výroky**. Pravdivostná hodnota pravdivého výroku je 1, pravdivostná hodnota nepravdivého výroku je 0.

Na označenie pravdivostnej hodnoty výroku A budeme používať symbol $\text{ph}(A)$.

PRÍKLAD 1.12. V teórii prirodzených čísel je veta „Súčet čísla dva a čísla tri je číslo päť.“ pravdivým výrok. „Tri je párne číslo.“ je nepravdivý výrok. „Číslo x je nepárne číslo.“ nie je výrok, lebo táto veta nie je ani pravdivá, ani nepravdivá. Pravdivou alebo nepravdivou sa stane až po dosadení konkrétneho čísla za x a to už bude iná veta. Veta „Číslo tri je nepárne číslo.“ je pravdivý výrok. ■

Výroky môžeme spájať pomocou špeciálnych slovných spojení a vytvárať tak zložitejšie výroky, hovoríme im **zložené výroky**.

DEFINÍCIA 1.10. Ak A, B sú výroky, tak
negáciou výroku A nazývame výrok „Nie je pravda, že A “ a označujeme ho $\bar{A}$ alebo $\neg A$,
konjunkciou výrokov A, B nazývame výrok „ A a B “ a označujeme ho $A \wedge B$,
disjunkciou výrokov A, B nazývame výrok „ A alebo B “ a označujeme ho $A \vee B$,
implikáciou výrokov A, B nazývame výrok „Ak A , potom B “ a označujeme ho $A \Rightarrow B$,
ekvivalenciou výrokov A, B nazývame výrok „ A vtedy a len vtedy, keď B “ a označujeme ho $A \Leftrightarrow B$.

Okrem uvedených slovných spojení sa pri vytváraní zložených výrokov používajú aj iné. Napríklad, ak A je výrok „Číslo 2 je väčšie ako 3.“, tak jeho negáciu $\bar{A}$ môžeme vyjadriť: „Nie je pravda, že číslo 2 je väčšie ako 3.“ alebo „Číslo 2 nie je väčšie ako 3.“ alebo „Číslo 2 je menšie alebo sa rovná číslu 3.“ Tieto tri výroky samozrejme považujeme za rovnaké.

Konjunkciu dvoch výrokov A, B môžeme vyjadriť aj „ A a súčasne B .“, ich implikáciu zas „Ak A, B .“ alebo „Ak A , tak B .“.

Aký je súvis medzi pravdivostnými hodnotami výrokov A, B a pravdivostnými hodnotami výrokov $\bar{A}, A \wedge B, A \vee B, A \Rightarrow B, A \Leftrightarrow B$? Pri ich určovaní sa vychádzalo zo zaužívaných spôsobov hodnotenia myslenia. Napríklad, ak výrok A je pravdivý, tak na otázku „Je pravdivý výrok A alebo B ?“ odpovieme „Áno, je pravdivý.“. Teda $ph(A \vee B) = 1$, keď $ph(A) = 1$. Pravdivostné hodnoty negácie, konjunkcie, disjunkcie, implikácie a ekvivalencie uvádzame v tab. 1.

TABUĽKA 1. Pravdivostné hodnoty zložených výrokov

A	$\bar{A}$	A	B	$A \wedge B$	A	B	$A \vee B$	A	B	$A \Rightarrow B$	A	B	$A \Leftrightarrow B$
0	1	0	0	0	0	0	0	0	0	1	0	0	1
1	0	0	1	0	0	1	1	0	1	1	0	1	0
		1	0	0	1	0	1	1	0	0	1	0	0
		1	1	1	1	1	1	1	1	1	1	1	1

DEFINÍCIA 1.11. Tieto tabuľky sa nazývajú **pravdivostné tabuľky** postupne negácie, konjunkcie, disjunkcie, implikácie, ekvivalencie.

Znaky negácie, konjunkcie, disjunkcie, implikácie, ekvivalencie, t.j. znaky $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ a im zodpovedajúce slovné spojenia nazývame **logické spojky** alebo **funktory**.

Výroky A, B sa nazývajú **ekvivalentné**, ak $ph(A \Leftrightarrow B) = 1$.

Uvažujme teraz o výroku „Ak zajtra bude u nás pekne, tak pôjdeme k jazeru alebo pôjdeme do hory.“ Skladá sa z výrokov „Zajtra bude u nás pekne.“, „Zajtra pôjdeme k jazeru alebo pôjdeme do hory.“. Keby sme prvý výrok označili A , druhý B , tak pôvodný výrok je $A \Rightarrow B$. Ale druhý výrok sa zasa skladá s dvoch výrokov, a to „Zajtra pôjdeme k jazeru.“ a „Zajtra pôjdeme do hory.“. Keď ich označíme postupne C, D , tak pôvodný výrok môžeme zapísať v tvare $A \Rightarrow (C \vee D)$. Výroky A, C, D sa už ďalej nedajú rozkladať na jednoduchšie výroky.

DEFINÍCIA 1.12. Výroky, ktoré sa nedajú rozložiť na jednoduchšie výroky, alebo výroky ktoré vždy vystupujú ako celok, sa nazývajú **atomické** (alebo **atomárne**).

PRÍKLAD 1.13. „Číslo 12 delí číslo 24 a číslo 4 číslo 12, a preto číslo 4 delí číslo 24“ je výrok v teórii prirodzených čísel. Skladá sa z atomických výrokov „Číslo 12 delí číslo

24“, „Číslo 4 delí číslo 12“, „Číslo 4 delí číslo 24“. Ak by sme si označili tieto atomické výroky postupne A, B, C , môžeme pôvodný výrok zapísať $(A \wedge B) \Rightarrow C$. ■

3.2. Kvantifikované výroky.

Už sme spomenuli, že veta (výraz) „Číslo x je nepárne číslo.“ nie je výrok. Ale ak za x dosadíme konkrétne celé číslo, dostaneme výrok.

Výraz, ktorý obsahuje jednu alebo viac premenných, z ktorého po dosadení prípustných hodnôt za premenné vznikne výrok, sa nazýva **výroková forma**. Ak $A(x_1, \dots, x_k)$ je výroková forma k premenných $x_1, \dots, x_k$, tak množina k -tic prípustných hodnôt sa nazýva **definičný obor výrokovej formy** $A(x_1, \dots, x_k)$. Množina všetkých $(q_1, \dots, q_k)$ z definičného oboru D výrokovej formy $A(x_1, \dots, x_k)$, pre ktoré je výrok $A(q_1, \dots, q_k)$ pravdivý, sa nazýva **obor pravdivosti výrokovej formy** $A(x_1, \dots, x_k)$ a označuje sa $\{(x_1, \dots, x_k) \in D; A(x_1, \dots, x_k)\}$.

PRÍKLAD 1.14. $x^2 + y^2 \leq 0$ je výroková forma dvoch premenných x, y . Jej definičný obor je $\mathbf{R}^2$. Do oboru pravdivosti patrí len dvojica $(0, 0)$, teda

$$\{(x, y) \in \mathbf{R}^2; x^2 + y^2 \leq 0\} = \{(0, 0)\}.$$

Výrokové formy môžeme spájať pomocou logických spojok, a tak vytvárať nové výrokové formy.

PRÍKLAD 1.15. Negáciou výrokovej formy $x \geq 2$ s definičným oborom $\mathbf{R}$ je výroková forma $x < 2$ s rovnakým definičným oborom.

Konjunkciou výrokových foriem $x^2 - x - 6 = 0$, $x > 0$ je výroková forma $x^2 - x - 6 = 0 \wedge x > 0$. ■

Z výrokovej formy sa dá vytvoriť výrok aj iným spôsobom ako je dosadenie hodnôt za premenné. Môžeme vytvoriť výrok, v ktorom sa hovorí o počte prvkov, ktoré keď dosadíme za premenné do výrokovej formy, dostaneme pravdivý výrok. Takéto výroky nazývame **kvantifikované výroky**. Nech $A(x)$ je výroková forma jednej premennej x s definičným oborom D . Potom môžeme vytvoriť takéto kvantifikované výroky:

Existuje (existuje aspoň jedno) x , že $A(x)$.

Existujú aspoň štyri x , že $A(x)$.

Existuje najviac päť x , že $A(x)$.

Existujú práve tri x , že $A(x)$.

Pre všetky x (platí) $A(x)$.

Výrazy vytlačené polotučnou kurzívou sa nazývajú **kvantifikátory**. V matematike sa najčastejšie používajú prvý a posledný. Ten prvý sa nazýva **existenčný** (alebo **malý**) **kvantifikátor** a posledný **všeobecný** (alebo **veľký**) **kvantifikátor**.

Existenčný kvantifikátor sa označuje symbolom $\exists$ (otočené písmeno E). Kvantifikovaný výrok

„Existuje x , že $A(x)$.“

môžeme stručne zapísať

$$\exists x \in D A(x) \quad \text{alebo} \quad \exists_{x \in D} A(x)$$

Ak je známy obor premennej x , môžeme použiť aj zápis

$$\exists x A(x) \quad \text{alebo} \quad \exists_x A(x).$$

Všeobecný kvantifikátor sa označuje symbolom $\forall$ (otočené písmeno A). Kvantifikovaný výrok

„Pre všetky x $A(x)$.“

stručne zapisujeme

$$\forall x \in D \ A(x) \quad \text{alebo} \quad \forall_{x \in D} A(x)$$

alebo, ak je známy obor premennej x ,

$$\forall x \ A(x) \quad \text{alebo} \quad \forall_x A(x).$$

PRÍKLAD 1.16. Rozhodnite o pravdivosti výrokov

- (1) $\exists n \in \mathbf{Z} \ n^2 = 9$,
- (2) $\forall n \in \mathbf{Z} \ n^2 = 9$,
- (3) $\exists n \in \mathbf{Z} \ n^2 = 2$,
- (4) $\forall n \in \mathbf{Z} \ n^2 = 2$.

Riešenie. Prvý výrok je pravdivý, lebo pre $n = -3$ je $(-3)^2 = 9$.

Druhý výrok je nepravdivý, lebo rovnosť $n^2 = 9$ neplatí pre každé celé číslo n , napr. pre $n = 0$ je $n^2 = 0^2 = 0 \neq 9$.

Tretí aj štvrtý výrok sú nepravdivé, lebo len pre dve reálne čísla platí, že ich druhá mocnina je 2. Sú to čísla $\sqrt{2}$ a $-\sqrt{2}$, no ani jedno z nich nie je celé číslo. ■

Kvantifikované výroky môžeme vytvoriť aj z výrokových foriem dvoch, troch a viac premenných. Napr. výraz

$$\exists x \in \mathbf{Z} \ \forall y \in \mathbf{R} \ x + y^2 \leq -4$$

je výrok, ktorý čítame:

„Existuje celé číslo x tak, že pre všetky reálne čísla y je $x + y^2 \leq -4$.“

Výrok

$$\forall y \in \mathbf{R} \ \exists x \in \mathbf{Z} \ \forall z \in \mathbf{R} \ x + y^2 - z \leq -4$$

čítame

„Pre každé reálne číslo y existuje celé číslo x tak, že pre všetky reálne čísla z je $x + y^2 - z \leq -4$.“

Nech $A(x, y)$ je výroková forma definovaná pre $x \in D, y \in E$. Výraz $\forall x \in D \ A(x, y)$ resp. $\exists x \in D \ A(x, y)$ nie je výrok. Ak však za premennú y dosadíme konkrétny prvok množiny E , dostaneme výrok. Uvedené výrazy sú teda výrokové formy premennej y .

PRÍKLAD 1.17. Rozhodnite o pravdivosti výrokov

- (1) $\forall x \in \mathbf{R} \ \exists y \in \mathbf{R} \ x - y = 1$,
- (2) $\exists y \in \mathbf{R} \ \forall x \in \mathbf{R} \ x - y = 1$.

Riešenie.

(1) Nech x je ľubovoľné reálne číslo. K splneniu rovnosti $x - y = 1$ stačí zvoliť $y = x - 1$. Ku každému $x \in \mathbf{R}$ sme našli (teda existuje) $y \in \mathbf{R}$ ($y = x - 1$) tak, že platí $x - y = 1$. To znamená, že výrok je pravdivý.

(2) Malo by existovať y také, že pre všetky reálne čísla x je $x - y = 1$. Označme to číslo y_0 . Pokiaľ existuje, má preň platiť $x - y_0 = 1$ pre všetky $x \in \mathbf{R}$. Lenže pre $x = y_0$ platí $x - y_0 = y_0 - y_0 = 0 \neq 1$. Znamená to, že také y_0 neexistuje, a teda výrok je nepravdivý. ■

POZNÁMKA 1.3. Výroky z predchádzajúceho príkladu sa od seba líšia len poradím kvantifikátorov. Aby bol prvý výrok pravdivý, je potrebné, aby pre každé x existovalo y tak, že $x - y = 1$. Uvedomme si, že pre rôzne čísla x aj zodpovedajúce čísla y môžu byť rôzne. Naproti tomu, aby bol pravdivý druhý výrok, je potrebné, aby existovalo jedno

y tak, že pre všetky x je $x - y = 1$. Teda to y je pre všetky x stále to isté. Vidíme, že zmenou poradia malého a veľkého kvantifikátora dostávame odlišné výroky, ktoré nemusia byť ekvivalentné.

Poradie za sebou idúcich kvantifikátorov rovnakého typu (oba sú všeobecné alebo oba sú existenčné) môžeme meniť a výrok sa pritom nezmení. Preto aj výrazy $\forall x \in D \forall y \in D$ resp. $\exists x \in D \exists y \in D$ skrácujeme na $\forall x, y \in D$ resp. $\exists x, y \in D$.

Venujme sa teraz tomu, ako tvoriť negácie kvantifikovaných výrokov. Nech $A(x)$ je výroková forma definovaná na množine D . Negáciou výroku $\exists x \in D A(x)$ je výrok „Nie je pravda, že existuje $x \in D$, pre ktoré platí $A(x)$.“ To je to isté ako „Neexistuje $x \in D$, pre ktoré platí $A(x)$.“ a tiež ako „Pre všetky $x \in D$ platí negácia $A(x)$.“, čo môžeme zapísať takto: $\forall x \in D \overline{A(x)}$. Podobnými úvahami by sme utvorili aj negácie ďalších typov kvantifikovaných výrokov. Uvádžeme ich v tabuľke 2. Číslo k je tu jedno konkrétne ale ináč ľubovoľné prirodzené číslo väčšie ako 1.

TABUĽKA 2. Negácie kvantifikovaných výrokov

Výrok	Negácia výroku
$\exists x \in D A(x)$	$\forall x \in D \overline{A(x)}$
Existuje aspoň k prvkov x , že $A(x)$.	Existuje najviac $k - 1$ prvkov x , že $A(x)$.
Existuje najviac k prvkov x , že $A(x)$.	Existuje aspoň $k + 1$ prvkov x , že $A(x)$.
Existuje práve k prvkov x , že $A(x)$.	Existuje najviac $k - 1$ alebo aspoň $k + 1$ prvkov x , že $A(x)$.
$\forall x \in D A(x)$	$\exists x \in D \overline{A(x)}$

Negáciu výroku, ktorý obsahuje niekoľko malých a veľkých kvantifikátorov získame tak, že každý malý kvantifikátor zmeníme na veľký, veľký kvantifikátor zmeníme na malý a výrokovú formu negujeme.

PRÍKLAD 1.18. Napíšte negácie výrokov

- (1) $\exists y \in \mathbf{R} \forall x \in \mathbf{R} xy \leq y$,
- (2) $\forall x \in \mathbf{N}^+ \exists y \in \mathbf{N}^+ \exists z \in \mathbf{N}^+ x^2 + y^2 = z^2$.

Riešenie.

- (1) $\forall y \in \mathbf{R} \exists x \in \mathbf{R} xy > y$,
- (2) $\exists x \in \mathbf{N}^+ \forall y \in \mathbf{N}^+ \forall z \in \mathbf{N}^+ x^2 + y^2 \neq z^2$.

■

3.3. Výrokové formuly.

Výroková logika pri skúmaní pravdivostných hodnôt zložených výrokov si nevšima obsah jednotlivých atomických výrokov ale ich pravdivostnú hodnotu a tiež tvar (štruktúru) zloženého výroku. Preto je vhodné zaviesť **výrokové premenné** – premenné, za ktoré je možné dosadzovať výroky – a pomocou nich, logických spojok a zátvoriek vytvárať výrazy, ktoré majú vlastnosť, že keď do nich za výrokové premenné dosadíme výroky, vzniknú z týchto výrazov výroky. Ako výrokové premenné budeme používať písmená p, q, r, s, t , poprípade tieto písmená s indexami napr. p_1, p_2, q_4 . Výrazy, o ktorých sme teraz hovorili, nazývame výrokové formuly. Ich presná definícia je takáto:

DEFINÍCIA 1.13. **Formula výrokového počtu** (skrátene **výroková formula** alebo **formula**) je každé slovo nad abecedou $\{ \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, (,), p, q, r, s, t, p_1, q_1, r_1, s_1, t_1, \dots \}$, ktoré vzniklo podľa pravidiel:

- (1) Každá výroková premenná je formula.
- (2) Ak a, b sú formuly, tak

$$\bar{a}, (a \wedge b), (a \vee b), (a \Rightarrow b), (a \Leftrightarrow b)$$

sú formuly.

- (3) Žiadne iné slová nie sú formuly.

Formulu $\bar{a}$ nazývame **negáciou formuly** a , formulu $(a \wedge b)$ nazývame **konjunkciou formúl** a, b , formulu $(a \vee b)$ nazývame **disjunkciou formúl** a, b , formulu $(a \Rightarrow b)$ nazývame **implikáciou formúl** a, b a formulu $(a \Leftrightarrow b)$ **ekvivalenciou formúl** a, b .

PRÍKLAD 1.19. p, q, r sú výrokové premenné, a teda aj formuly, preto $(p \Rightarrow q), (p \vee r)$ sú tiež formuly. Keď použijeme opakovane postup z bodu 2 definície formuly, tak dostaneme aj tieto formuly: $(p \Rightarrow (q \vee r)), ((p \wedge \bar{q}) \Rightarrow (r \Rightarrow (r \Rightarrow q)))$. ■

Keby sme v definícii formuly nepoužili zátvorky, tak by formuly z predchádzajúceho príkladu mali tvar $p \Rightarrow q, p \vee r$, ale už pri posledných dvoch formulách $p \Rightarrow q \vee r, p \wedge \bar{q} \Rightarrow r \Rightarrow r \Rightarrow q$ by sme po dosadení výrokov za výrokové premenné mohli dostať vetu, ktorá nie je po obsahovej stránke jednoznačná a teda nie je výrok. Napríklad veta „Keď Vlado hovorí, vtedy Jano mlčí alebo Ivan plače“ vznikne dosadením do $p \Rightarrow (q \vee r)$, ale tiež do $(p \Rightarrow q) \vee r$. V hovorovej reči sa obvykle používajú nepísané dohody a väčšina by túto vetu priradila k $p \Rightarrow (q \vee r)$ a nie k $(p \Rightarrow q) \vee r$. V matematike, ale aj iných odboroch, je takáto nejednoznačnosť neprípustná.

Situácia, aby veľa zátvoriek nebolo na ujmu prehľadnosti, ale pritom nevznikala nejednoznačnosť, sa rieši buď

- dohodou, že zátvorky vynechávame, keď nemôže prísť k nejednoznačnosti alebo
- dohodou o vynechávaní zátvoriek a priority logických spojok.

Dohoda o vonkajších zátvorkách: V samostatne stojacich formulách budeme vonkajšie zátvorky vynechávať.

Princíp priority logických spojok: Ak logické spojky usporiadame do postupnosti $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$, tak každá logická spojka, stojaca vľavo od uvažovanej, viaže silnejšie. Nech p, q, r sú výrokové premenné. Logická spojka L **viaže silnejšie** ako logická spojka K znamená, že $p L q K r$ je formula $(p L q) K r$.

Poznamenajme, že tento princíp poznáme z reálnych čísel, kde „krát“ viaže silnejšie ako „plus“, čiže napr. $2.3 + 1$ znamená $(2.3) + 1$ a nie $2.(3 + 1)$.

PRÍKLAD 1.20.

- $p \wedge q \vee \bar{r}$ znamená formulu $(p \wedge q) \vee \bar{r}$,
- $p \Rightarrow q \vee r \Leftrightarrow p$ znamená formulu $(p \Rightarrow (q \vee r)) \Leftrightarrow p$,
- $p \vee r \Leftrightarrow p \wedge q \vee r$ znamená formulu $(p \vee r) \Leftrightarrow ((p \wedge q) \vee r)$. ■

DEFINÍCIA 1.14. Postupnosť formúl $a_1, a_2, \dots, a_n$ sa nazýva **vytvárajúca postupnosť formuly** a , ak $a = a_n$ a pre každé $k \in \{1, 2, \dots, n\}$ je a_k buď výroková premenná alebo existujú $i, j \in \{1, 2, \dots, k-1\}$ tak, že a_k je jedna z formúl $\bar{a}_i, a_i \wedge a_j, a_i \vee a_j, a_i \Rightarrow a_j, a_i \Leftrightarrow a_j$.

PRÍKLAD 1.21. Vytvárajúcou postupnosťou formuly

$$a = ((p \vee \bar{q}) \wedge \overline{\bar{p} \vee r}) \Rightarrow (p \Rightarrow (q \Rightarrow r))$$

je postupnosť $p, q, r, \bar{p}, \bar{q}, p \vee \bar{q}, \bar{p} \vee r, \overline{\bar{p} \vee r}, q \Rightarrow r, (p \vee \bar{q}) \wedge \overline{\bar{p} \vee r}, p \Rightarrow (q \Rightarrow r), ((p \vee \bar{q}) \wedge \overline{\bar{p} \vee r}) \Rightarrow (p \Rightarrow (q \Rightarrow r))$. ■

DEFINÍCIA 1.15. Ak formula b obsahuje výrokové premenné $p_1, p_2, \dots, p_n$ a žiadne iné, tak formulu b označíme $b(p_1, p_2, \dots, p_n)$ a hovoríme, že b je formula n premenných $p_1, p_2, \dots, p_n$.

DEFINÍCIA 1.16. Výrok, ktorý vznikne z formuly, keď za všetky jej výrokové premenné dosadíme výroky, sa nazýva **interpretácia formuly**.

POZNÁMKA 1.4. Ak $A_1, \dots, A_n$ sú výroky a $b(p_1, p_2, \dots, p_n)$ je formula, tak dosadením výroku A_1 za premennú p_1 , A_2 za p_2 až A_n za p_n dostaneme výrok $b(A_1, A_2, \dots, A_n)$, ktorý je interpretáciou formuly b .

PRÍKLAD 1.22. Vezmime formulu $r \wedge s \Rightarrow t$. Jej interpretácie v teórii prirodzených čísel sú napríklad:

„Keď 2 delí 12 aj 3 delí 12, tak aj 6 delí 12.“

„Ak číslo 3 je väčšie ako číslo 2 a číslo 7 je väčšie ako číslo 32, tak číslo 3 je väčšie ako číslo 32.“

„Ak 5 je menšie ako 6 a 15 je väčšie ako 13, tak 5 je menšie ako 3.“

Formula $r \wedge s \Rightarrow t$ je formulou troch premenných r, s, t , môžeme ju teda označiť napr. $a(r, s, t)$. ■

Výroková formula nie je výrok, nemá teda pravdivostnú hodnotu. Každý výrokovej formule $a(p_1, p_2, \dots, p_n)$ však môžeme priradiť funkciu, ktorá vyjadruje závislosť pravdivostných hodnôt interpretácií $a(A_1, A_2, \dots, A_n)$ tejto formuly od pravdivostných hodnôt výrokov A_1, A_2 až A_n dosadených za jednotlivé výrokové premenné.

DEFINÍCIA 1.17. Nech $a(p_1, p_2, \dots, p_n)$ je formula n premenných. Funkcia

$$\text{ph}_a : \{0, 1\}^n \rightarrow \{0, 1\}, \text{ph}_a(x_1, x_2, \dots, x_n) = \text{ph}(a(A_1, A_2, \dots, A_n)),$$

kde $A_1, A_2, \dots, A_n$ sú výroky, pre ktoré $\text{ph}(A_1) = x_1, \text{ph}(A_2) = x_2, \dots, \text{ph}(A_n) = x_n$, sa nazýva **pravdivostné ohodnotenie formuly** a .

Všetkých usporiadaných n -tíc prvkov 0, 1 je 2^n . Označme ich $\beta_1 = (0, 0, \dots, 0, 0)$, $\beta_2 = (0, 0, \dots, 0, 1)$, $\beta_3 = (0, 0, \dots, 1, 0)$, $\dots$, $\beta_{2^n} = (1, 1, \dots, 1)$. Potom môžeme pravdivostné ohodnotenie formuly $a(p_1, p_2, \dots, p_n)$ zapísať v tvare tabuľky (pozri tab. 3), ktorú nazývame **pravdivostnou tabuľkou formuly** $a(p_1, p_2, \dots, p_n)$.

TABUĽKA 3. Pravdivostná tabuľka formuly a

$(p_1, p_2, \dots, p_n)$	$a(p_1, p_2, \dots, p_n)$
β_1	$\text{ph}_a(\beta_1)$
β_2	$\text{ph}_a(\beta_2)$
$\vdots$	$\vdots$
β_{2^n}	$\text{ph}_a(\beta_{2^n})$

PRÍKLAD 1.23. Pravdivostné tabuľky formúl

$$r \wedge \bar{s} \Leftrightarrow s \vee \bar{r}, (r \wedge s) \vee t \Rightarrow (s \Rightarrow t)$$

sú v tab. 4.

TABUĽKA 4

(r, s)	$r \wedge \bar{s} \Leftrightarrow s \vee \bar{r}$	(r, s, t)	$(r \wedge s) \vee t \Rightarrow (s \Rightarrow t)$
(0,0)	0	(0,0,0)	1
(0,1)	0	(0,0,1)	1
(1,0)	0	(0,1,0)	1
(1,1)	0	(0,1,1)	1
		(1,0,0)	1
		(1,0,1)	1
		(1,1,0)	0
		(1,1,1)	1

Pri ich tvorbe je vhodné postupovať tak, že do hlavičky tabuľky zapíšeme vytvárajúcu postupnosť danej formuly (pozri tab. 5 a 6), pod premenné dáme všetky možné zoskupenia pravdivostných hodnôt a postupne po stĺpcoch vyplňujeme pravdivostné ohodnotenia jednotlivých formúl vytvárajúcej postupnosti na základe pravdivostných tabuliek zložených výrokov (tab. 1). ■

TABUĽKA 5

r, s	$\bar{s}$	$r \wedge \bar{s}$	$\bar{r}$	$s \vee \bar{r}$	$(r \wedge \bar{s}) \Leftrightarrow (s \vee \bar{r})$
0,0	1	0	1	1	0
0,1	0	0	1	1	0
1,0	1	1	0	0	0
1,1	0	0	0	1	0

TABUĽKA 6

r, s, t	$r \wedge s$	$(r \wedge s) \vee t$	$s \Rightarrow t$	$(r \wedge s) \vee t \Rightarrow (s \Rightarrow t)$
0,0,0	0	0	1	1
0,0,1	0	1	1	1
0,1,0	0	0	0	1
0,1,1	0	1	1	1
1,0,0	0	0	1	1
1,0,1	0	1	1	1
1,1,0	1	1	0	0
1,1,1	1	1	1	1

DEFINÍCIA 1.18. Formula sa nazýva **tautológia**, ak jej pravdivostným ohodnotením je konštantná funkcia s hodnotou 1; **kontradikcia**, ak jej pravdivostným ohodnotením je konštantná funkcia s hodnotou 0; **splniteľná**, ak nie je kontradikciou.

PRÍKLAD 1.24.

Formula $p \vee \bar{p}$ je tautológia.

Formula $p \wedge \bar{p}$ je kontradikcia.

Formula $p \Rightarrow q$ je splniteľná.

Formula $(p \wedge (p \Rightarrow q)) \Rightarrow q$ je tautológia.

Výsledok vidíme z tab. 7. ■

TABUĽKA 7

p	$\bar{p}$	$p \vee \bar{p}$	$p \wedge \bar{p}$
0	1	1	0
1	0	1	0

$p \ q$	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
0 0	1	0	1
0 1	1	0	1
1 0	0	0	1
1 1	1	1	1

Tautológia $(p \wedge (p \Rightarrow q)) \Rightarrow q$ je základom pre správne usudzovanie. Ukazuje nám, ako z pravdivosti jedného výroku usúdiť, že je pravdivý druhý výrok. Z pravdivostnej tabuľky tejto formuly vidieť, že keď A, B sú výroky, pričom výroky $A, A \Rightarrow B$ sú pravdivé, potom je pravdivý aj výrok B . Na usúdenie pravdivosti výroku B nepostačuje len pravdivosť implikácie $A \Rightarrow B$. Vidieť to z prvého riadku pravdivostnej tabuľky formuly $p \Rightarrow q$. Výrok $A \Rightarrow B$ môže byť pravdivý a pritom výrok B je nepravdivý.

DEFINÍCIA 1.19. Dve formuly a, b s rovnakými premennými sa nazývajú **tautologicky ekvivalentné**, ak majú rovnaké pravdivostné ohodnotenie. Tautologicky ekvivalentné formuly označujeme $a \sim b$.

PRÍKLAD 1.25. Dokážte, že formuly $\overline{p \wedge q}$ a $\bar{p} \vee \bar{q}$ sú tautologicky ekvivalentné.

Riešenie. Napíšeme pravdivostné tabuľky (tab. 8) týchto formúl. Obidve formuly majú dve premenné, a to p, q . Tabuľkami sú definované rovnaké funkcie, teda formuly sú tautologicky ekvivalentné. ■

TABUĽKA 8

$p \ q$	$\overline{p \wedge q}$
0 0	1
0 1	1
1 0	1
1 1	0

$p \ q$	$\bar{p} \vee \bar{q}$
0 0	1
0 1	1
1 0	1
1 1	0

PRÍKLAD 1.26. Zistite, či platí $(p \vee q) \vee r \sim p \vee (q \vee r)$.

Riešenie. Urobíme pomocnú tabuľku (tab. 9) a z nej už bude vidieť, keď si pozrieme prvý, predposledný a posledný stĺpec, či formuly majú rovnaké pravdivostné ohodnotenie. ■

TABUĽKA 9

p, q, r	$p \vee q$	$q \vee r$	$(p \vee q) \vee r$	$p \vee (q \vee r)$
0, 0, 0	0	0	0	0
0, 0, 1	0	1	1	1
0, 1, 0	1	1	1	1
0, 1, 1	1	1	1	1
1, 0, 0	1	0	1	1
1, 0, 1	1	1	1	1
1, 1, 0	1	1	1	1
1, 1, 1	1	1	1	1

V nasledujúcej vete uvedieme základné tautologické ekvivalencie.

VETA 1.2. Nech a, b, c sú formuly s rovnakými premennými. Potom platia tieto tautologické ekvivalencie:

- | | | |
|------|--|--|
| E1. | $a \vee b \sim b \vee a,$ | $a \wedge b \sim b \wedge a,$ |
| E2. | $(a \vee b) \vee c \sim a \vee (b \vee c),$ | $(a \wedge b) \wedge c \sim a \wedge (b \wedge c),$ |
| E3. | $(a \vee b) \wedge c \sim (a \wedge c) \vee (b \wedge c),$ | $(a \wedge b) \vee c \sim (a \vee c) \wedge (b \vee c),$ |
| E4. | $\overline{a \vee b} \sim \overline{a} \wedge \overline{b},$ | $\overline{a \wedge b} \sim \overline{a} \vee \overline{b},$ |
| E5. | $a \vee a \sim a,$ | $a \wedge a \sim a,$ |
| E6. | $a \vee (b \wedge \overline{b}) \sim a,$ | $a \wedge (b \vee \overline{b}) \sim a,$ |
| E7. | $\overline{\overline{a}} \sim a,$ | |
| E8. | $a \vee (a \wedge b) \sim a,$ | $a \wedge (a \vee b) \sim a,$ |
| E9. | $a \Rightarrow b \sim \overline{a} \vee b,$ | $a \Rightarrow b \sim \overline{a \wedge \overline{b}},$ |
| E10. | $a \Leftrightarrow b \sim (\overline{a} \vee b) \wedge (a \vee \overline{b}),$ | $a \Leftrightarrow b \sim (a \wedge b) \vee (\overline{a} \wedge \overline{b}).$ |

Dôkaz tejto vety neurobíme, necháme na čitateľa, aby urobil a porovnal príslušné pravdivostné tabuľky. $\square$

PRÍKLAD 1.27. Dokážte $p \Rightarrow q \sim \overline{p \wedge \overline{q}}$, druhú z ekvivalencií E9 z predchádzajúcej vety.

Riešenie. Uvedený vzťah môžeme dokázať buď pomocou pravdivostných tabuliek oboch formúl, alebo využitím tabuľky tautologických ekvivalencií. Použijeme tautologické ekvivalencie. Nad znak tautologickej ekvivalencie napíšeme ktoré pravidlo z tabuľky tautologických ekvivalencií sme použili. Z E9 sme použili prvú ekvivalenciu.

$$p \Rightarrow q \stackrel{E9}{\sim} \overline{p} \vee q \stackrel{E7}{\sim} \overline{\overline{\overline{p} \vee q}} \stackrel{E4}{\sim} \overline{p \wedge \overline{q}}$$

■

DEFINÍCIA 1.20. Hovoríme, že množina logických spojok S je **úplný systém logických spojok** (skrátene USLS), ak pre každú formulu a existuje formula b , ktorá obsahuje iba logické spojky z množiny S a platí $a \sim b$. Vtedy tiež hovoríme, že formula a **sa dá vyjadriť pomocou S** .

PRÍKLAD 1.28. Ukážte, že množiny $\{\vee, \wedge, \neg\}$, $\{\neg, \Rightarrow\}$ sú úplné systémy logických spojok.

Riešenie. Pre každé formuly c, d platí

$$\begin{aligned} c &\Rightarrow d \sim \bar{c} \vee d, \\ c &\Leftrightarrow d \sim (\bar{c} \vee d) \wedge (c \vee \bar{d}). \end{aligned}$$

Pomocou týchto ekvivalencií môžeme každú formulu a upraviť na ekvivalentnú formulu b , ktorá neobsahuje logické spojky $\Rightarrow, \Leftrightarrow$, teda obsahuje iba logické spojky z množiny $\{\vee, \wedge, \neg\}$. Tým sme dokázali, že $\{\vee, \wedge, \neg\}$ je USLS.

Aby sme dokázali, že $\{\neg, \Rightarrow\}$ je USLS, stačí dokázať, že každá formula a , ktorá obsahuje logické spojky len z množiny $\{\vee, \wedge, \neg\}$ je ekvivalentná niektorej formule b , ktorá obsahuje logické spojky len z množiny $\{\neg, \Rightarrow\}$. Pravdivosť tohto tvrdenia vyplýva z toho, že pre každé formuly c, d platí

$$\begin{aligned} c \vee d &\sim \bar{c} \Rightarrow d, \\ c \wedge d &\sim \overline{\bar{c} \wedge \bar{d}} \sim \overline{\bar{c} \vee \bar{d}} \sim \overline{c \Rightarrow d}. \end{aligned}$$

■

PRÍKLAD 1.29. Vyjadrite formulu $p \Leftrightarrow q$ pomocou

- a) $\{\vee, \wedge, \neg\}$,
- b) $\{\neg, \Rightarrow\}$.

Riešenie.

a) $p \Leftrightarrow q \sim (p \Rightarrow q) \wedge (q \Rightarrow p) \sim (\bar{p} \vee q) \wedge (p \vee \bar{q}).$

b) Použijeme $c \wedge d \sim \overline{\bar{c} \vee \bar{d}} \sim \overline{c \Rightarrow d}$. Potom platí

$$p \Leftrightarrow q \sim (p \Rightarrow q) \wedge (q \Rightarrow p) \sim \overline{(p \Rightarrow q) \Rightarrow \overline{q \Rightarrow p}}.$$

■

4. Relácie

DEFINÍCIA 1.21. **Binárnou reláciou** (stručne len **reláciou**) **na množine** A nazývame ľubovoľnú podmnožinu karteziánskeho súčinu A^2 .

POZNÁMKA 1.5. Ak $\sigma \subset A^2$ je binárna relácia na množine A a $(x, y) \in \sigma$, tak hovoríme, že **prvok** x **je v relácii** σ **s prvkom** y a namiesto $(x, y) \in \sigma$ píšeme aj $x \sigma y$.

DEFINÍCIA 1.22. Relácia σ na množine A sa nazýva
reflexívna, ak $\forall x \in A \ (x, x) \in \sigma$,
symetrická, ak $\forall x, y \in A \ (x, y) \in \sigma \Rightarrow (y, x) \in \sigma$,
antisymetrická, ak $\forall x, y \in A \ (x, y) \in \sigma \wedge (y, x) \in \sigma \Rightarrow x = y$,
tranzitívna, ak $\forall x, y, z \in A \ (x, y) \in \sigma \wedge (y, z) \in \sigma \Rightarrow (x, z) \in \sigma$.

PRÍKLAD 1.30. Zistite, či relácia $\sigma \subset \mathbf{R}^2$, $\sigma = \{(x, y) ; x \leq y\}$ je reflexívna, symetrická, antisymetrická, tranzitívna.

Riešenie. Relácia σ je reflexívna, lebo pre každé $x \in \mathbf{R}$ platí $x \leq x$, teda $(x, x) \in \sigma$. Relácia nie je symetrická, pretože napríklad $(2, 3) \in \sigma$, ale $(3, 2) \notin \sigma$. Relácia je antisymetrická: Nech $(x, y) \in \sigma$, $(y, x) \in \sigma$, teda $x \leq y$, $y \leq x$. Z vlastností reálnych čísel vieme, že potom platí $x = y$. Relácia je tranzitívna: Ak $(x, y) \in \sigma$ a zároveň $(y, z) \in \sigma$, teda $x \leq y$ a zároveň $y \leq z$, potom z vlastností reálnych čísel vyplýva $x \leq z$, teda $(x, z) \in \sigma$. ■

DEFINÍCIA 1.23. Binárna relácia na množine A , ktorá je reflexívna, symetrická a tranzitívna, sa nazýva **ekvivalencia** alebo **relácia ekvivalencie** na množine A .

PRÍKLAD 1.31. Je relácia $\varrho = \{(x, y) \in \mathbf{Z}^2; 3 \mid (y - x)\}$ ekvivalenciou na množine $\mathbf{Z}$ všetkých celých čísel? ($a \mid b$ znamená: číslo b je deliteľné číslom a .)

Riešenie. $x - x = 0$, čo je číslo deliteľné tromi, preto $(x, x) \in \varrho$. Relácia ϱ je teda reflexívna.

Nech $(x, y) \in \varrho$. To znamená, že 3 delí číslo $y - x$. V takom prípade $y - x = 3k$, kde $k \in \mathbf{Z}$. Potom $x - y = -(y - x) = 3(-k)$, čo znamená, že $3 \mid (x - y)$ a teda $(y, x) \in \varrho$. Z toho vyplýva, že relácia ϱ je symetrická.

Nech $(x, y), (y, z) \in \varrho$. Existujú teda také celé čísla m, n , že $y - x = 3m, z - y = 3n$. Potom $z - x = z - x - y + y = (z - y) + (y - x) = 3m + 3n = 3(m + n)$. Číslo $z - x$ je deliteľné číslom 3, to znamená $(x, z) \in \varrho$ a teda relácia ϱ je tranzitívna.

Relácia ϱ má požadované vlastnosti, je preto ekvivalenciou na množine $\mathbf{Z}$. ■

POZNÁMKA 1.6. Ak ϱ je relácia ekvivalencie a $(x, y) \in \varrho$, tak budeme hovoriť, že x **je ekvivalentné s** y .

DEFINÍCIA 1.24. Nech σ je relácia ekvivalencie na množine A a $a \in A$. Potom množinu $\sigma(a) = \{x \in A; a \sigma x\}$ nazývame **triedou ekvivalencie prvku** a .

PRÍKLAD 1.32. Pre reláciu ekvivalencie ϱ definovanú v predchádzajúcom príklade nájdime triedy ekvivalencie prvkov 0, 1, 2.

Riešenie.

$$\begin{aligned}\varrho(0) &= \{x \in \mathbf{Z}; 0 \varrho x\} = \{x \in \mathbf{Z}; 3 \mid (x - 0)\} = \{x; x = 3k, k \in \mathbf{Z}\} = \{3k; k \in \mathbf{Z}\}, \\ \varrho(1) &= \{x \in \mathbf{Z}; 1 \varrho x\} = \{x \in \mathbf{Z}; 3 \mid (x - 1)\} = \{x; x = 3k + 1, k \in \mathbf{Z}\} = \{3k + 1; k \in \mathbf{Z}\}, \\ \varrho(2) &= \{x \in \mathbf{Z}; 2 \varrho x\} = \{x \in \mathbf{Z}; 3 \mid (x - 2)\} = \{x; x = 3k + 2, k \in \mathbf{Z}\} = \{3k + 2; k \in \mathbf{Z}\}. \blacksquare\end{aligned}$$

VETA 1.3. Nech σ je relácia ekvivalencie na množine A . Potom pre každé $x, y \in A$

- (1) $x \in \sigma(x)$,
- (2) $x \in \sigma(y)$ práve vtedy, keď $\sigma(x) = \sigma(y)$,
- (3) ak $\sigma(x) \neq \sigma(y)$, tak $\sigma(x) \cap \sigma(y) = \emptyset$.

Dôkaz.

(1) Relácia σ je reflexívna, preto pre každé $x \in A$ platí $(x, x) \in \sigma$, čo znamená, že $x \in \sigma(x)$.

(2) Nech $x \in \sigma(y)$ t.j. $(y, x) \in \sigma$. Ukážeme, že každý prvok $z \in \sigma(x)$ je prvkom aj množiny $\sigma(y)$. Nech teda $z \in \sigma(x)$, čo znamená, že $(x, z) \in \sigma$. Keďže $(y, x) \in \sigma$ a súčasne $(x, z) \in \sigma$, z tranzitívnosti relácie σ vyplýva $(y, z) \in \sigma$, a teda $z \in \sigma(y)$. Ukázali sme, že $\sigma(x) \subset \sigma(y)$. Analogicky sa ukáže, že $\sigma(y) \subset \sigma(x)$. Potom však platí $\sigma(x) = \sigma(y)$.

(3) (nepriamo) Nech $\sigma(x) \cap \sigma(y) \neq \emptyset$. Potom existuje $z \in \sigma(x) \cap \sigma(y)$ a pre tento prvok platí $(x, z) \in \sigma, (y, z) \in \sigma$. Keďže relácia σ je symetrická a tranzitívna, tak $(x, y) \in \sigma$ čiže $x \in \sigma(y)$ a podľa (2) $\sigma(x) = \sigma(y)$, čo je spor. □

PRÍKLAD 1.33. V relácii ekvivalencie $\varrho = \{(x, y) \in \mathbf{Z}^2; 3 \mid (y - x)\}$ jedinými triedami ekvivalencie sú $\varrho(0) = \{3k; k \in \mathbf{Z}\}$, $\varrho(1) = \{3k + 1; k \in \mathbf{Z}\}$, $\varrho(2) = \{3k + 2; k \in \mathbf{Z}\}$, lebo ľubovoľné celé číslo má tvar $3m, 3m + 1$ alebo $3m + 2$ ($m \in \mathbf{Z}$) a potom $\varrho(3m) = \varrho(0)$, lebo $3m \in \varrho(0)$; $\varrho(3m + 1) = \varrho(1)$, lebo $3m + 1 \in \varrho(1)$; $\varrho(3m + 2) = \varrho(2)$, lebo $3m + 2 \in \varrho(2)$. ■

DEFINÍCIA 1.25. Nech A je neprázdna množina a T je systém podmnožín množiny A , pre ktorý platí

- (1) $\forall X \in T \quad X \neq \emptyset$,
- (2) $\forall X, Y \in T \quad X \neq Y \Rightarrow X \cap Y = \emptyset$,

$$(3) \bigcup_{X \in T} X = A.$$

Potom T sa nazýva **rozklad množiny** A a prvky množiny T sa nazývajú **triedy rozkladu množiny** A .

PRÍKLAD 1.34. Nech $A = \{a, b, c, d, e\}$, $A_1 = \{a\}$, $A_2 = \{b, d, e\}$, $A_3 = \{c\}$, $B_1 = \{a, b, c\}$, $B_2 = \{b, d, e\}$. Potom $T = \{A_1, A_2, A_3\}$ je rozklad množiny A , lebo množiny A_1 , A_2 , A_3 sú neprázdne, prienik každých dvoch rôznych z nich je prázdna množina a zjednotenie všetkých troch množín je množina A . Naproti tomu $S = \{B_1, B_2\}$ nie je rozklad množiny A , lebo $B_1 \neq B_2$ ale $B_1 \cap B_2 = \{b\} \neq \emptyset$. ■

PRÍKLAD 1.35. Triedy ekvivalencie $\varrho(0)$, $\varrho(1)$, $\varrho(2)$ relácie ekvivalencie $\varrho = \{(x, y) \in \mathbf{Z}^2; 3 \mid (y - x)\}$ tvoria rozklad množiny $\mathbf{Z}$, pretože $\varrho(0) = \{0, \pm 3, \pm 6, \dots\}$, $\varrho(1) = \{1, -2, 4, -5, 7, -8, 10, \dots\}$, $\varrho(2) = \{2, -1, 5, -4, 8, -7, 11, \dots\}$, čo sú neprázdne množiny, $\varrho(0) \cap \varrho(1) = \emptyset$, $\varrho(0) \cap \varrho(2) = \emptyset$, $\varrho(1) \cap \varrho(2) = \emptyset$ a $\varrho(0) \cup \varrho(1) \cup \varrho(2) = \mathbf{Z}$. ■

VETA 1.4. Nech σ je ekvivalencia na množine A . Potom triedy ekvivalencie $\sigma(a)$, pre $a \in A$ tvoria rozklad množiny A . Triedami rozkladu sú triedy ekvivalencie relácie σ .

Dôkaz. Z vety 1.3 vyplýva, že každá trieda ekvivalencie $\sigma(a)$ prvku $a \in A$ je neprázdna, lebo $a \in A$. V tretej vlastnosti tejto vety sa priamo hovorí, že prienik dvoch rôznych tried ekvivalencie je prázdna množina. Každá trieda ekvivalencie obsahuje len prvky množiny A , preto $\bigcup_{a \in A} \sigma(a) \subset A$. Na druhej strane pre ľubovoľný prvok $b \in A$ platí $b \in \sigma(b)$, a teda

$$A \subset \bigcup_{a \in A} \sigma(a). \quad \text{V spojení s predchádzajúcou inklúziou dostávame}$$

$$\bigcup_{a \in A} \sigma(a) = A. \quad \square$$

POZNÁMKA 1.7. O rozklade, ktorý je tvorený triedami ekvivalencie, hovoríme, že je to **rozklad indukovaný** danou **ekvivalenciou**.

VETA 1.5. Ku každému rozkladu množiny A existuje jednoznačne určená ekvivalencia na množine A , ktorá tento rozklad indukuje.

Dôkaz. 1. Nech T je rozklad množiny A . Definujme na množine A reláciu σ takto:

$$a \sigma b \text{ práve vtedy, keď existuje } X \in T \text{ také, že } a, b \in X.$$

Je zrejmé, že táto relácia je reflexívna, symetrická a tranzitívna. Teda je to ekvivalencia. Ďalej vidíme, že prvky patriace do jednej triedy rozkladu sú navzájom ekvivalentné. Preto každá trieda rozkladu X je podmnožinou jednej triedy ekvivalencie relácie σ . Táto trieda ekvivalencie už nemôže obsahovať ďalšiu triedu rozkladu Y ($Y \neq X$), lebo v opačnom prípade by pre prvky $x \in X, y \in Y$ na základe definície relácie σ platilo $(x, y) \notin \sigma$ a na druhej strane $(x, y) \in \sigma$, pretože x aj y patria do tej istej triedy ekvivalencie, a to je spor. Tým sme ukázali, že každá trieda rozkladu T je triedou ekvivalencie σ .

2. Z časti 1 vyplýva, že existuje aspoň jedna ekvivalencia, ktorá indukuje rozklad množiny A , ktorý je zhodný s T . Teraz ukážeme, že táto ekvivalencia je jediná.

Predpokladajme, že existuje ešte jedna ekvivalencia $\tau \subset A \times A$ na množine A , ktorou indukovaný rozklad množiny A na triedy ekvivalencie je opäť T .

Nech $a \tau b$. Teda existuje $X \in T$ také, že $X = \tau(a) = \tau(b)$. To znamená, že $a, b \in X$, a teda $a \sigma b$, kde σ je ekvivalencia z prvej časti dôkazu. Z toho vyplýva, že podmienka $(a, b) \in \tau$ implikuje $(a, b) \in \sigma$, a teda $\tau \subset \sigma$.

Nech naopak $(a, b) \in \sigma$. Teda existuje $X \in T$ také, že $a, b \in X$. Ale pretože T je rozklad

indukovaný aj ekvivalenciou τ , X je jednou z tried ekvivalencie τ . Preto $(a, b) \in \tau$. Z toho vyplýva, že $\sigma \subset \tau$, a teda spolu s predošlou časťou dostávame $\sigma = \tau$. Tým je veta dokázaná. $\square$

Dokázali sme, že medzi ekvivalenciami na množine A a rozkladmi množiny A je vzájomne jedno-jednoznačné priradenie. Túto skutočnosť budeme využívať tak, že ekvivalenciu budeme definovať pomocou k nej patriaceho rozkladu.

PRÍKLAD 1.36. Nech systém množín $T = \{\{a, b, c\}, \{d, e\}, \{f\}\}$ je rozklad množiny $A = \{a, b, c, d, e, f\}$. Potom relácia ekvivalencie σ , ktorá tento rozklad indukuje, je $\sigma = \{(a, a), (b, b), (c, c), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b), (d, d), (e, e), (d, e), (e, d), (f, f)\}$. Vidíme, že zápis ekvivalencie pomocou príslušného rozkladu je oveľa prehľadnejší. $\blacksquare$

5. Orientované grafy

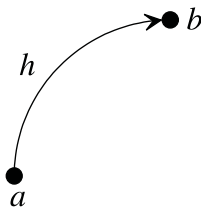
Teraz uvedieme základné pojmy z teórie grafov, ktoré využijeme pri štúdiu teórie konečných automatov.

DEFINÍCIA 1.26. ***Orientovaný graf*** je usporiadaná trojica $G = (V, H, e)$, kde V, H sú konečné množiny, $V \neq \emptyset, V \cap H = \emptyset$ a e je zobrazenie $e : H \rightarrow V^2$. Prvky množiny V sa nazývajú ***vrcholy***, prvky množiny H sa nazývajú ***orientované hrany*** a zobrazenie e sa nazýva ***incidencia***. Ak u, v sú vrcholy, h je orientovaná hrana a $e(h) = (u, v)$, tak u, v sa nazývajú ***krajné vrcholy orientovanej hrany*** h , špeciálne: vrchol u sa nazýva ***začiatočný vrchol orientovanej hrany*** h a vrchol v ***koncový vrchol orientovanej hrany*** h .

PRÍKLAD 1.37. Nech $V = \{1, 2, 3, 4\}$, $H = \{h_1, h_2, h_3, h_4, h_5, h_6\}$ $e : e(h_1) = (1, 4)$, $e(h_2) = (4, 2)$, $e(h_3) = (3, 2)$, $e(h_4) = e(h_5) = (3, 4)$, $e(h_6) = (2, 2)$. Potom $G = (V, H, e)$ je orientovaný graf. $\blacksquare$

DEFINÍCIA 1.27. Grafy $G = (V, H, e), G' = (V', H', e')$ sú rovnaké, ak $V = V', H = H', e = e'$.

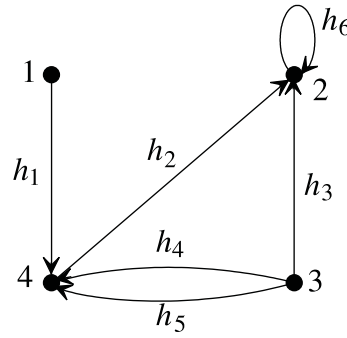
Orientované grafy budeme znázorňovať aj graficky a to takýmto spôsobom: vrcholy orientovaného grafu G znázorníme ako body roviny, ktoré označíme rovnako ako samotné vrcholy. Nech h je orientovaná hrana s krajnými vrcholmi a, b . Potom orientovanú hranu



OBR. 1

h s počiatočným vrcholom a a koncovým b znázorníme ako čiaru spájajúcu body a, b so šípkou pri koncovom vrchole b (obr. 1). Takto vytvorený objekt budeme nazývať ***diagram orientovaného grafu*** G . Často však namiesto „diagram grafu G “ budeme hovoriť iba „graf G “.

POZNÁMKA 1.8. Tu sa budeme zaoberať iba orientovanými grafmi, preto slovo orientovaný budeme často vynechávať.



OBR. 2

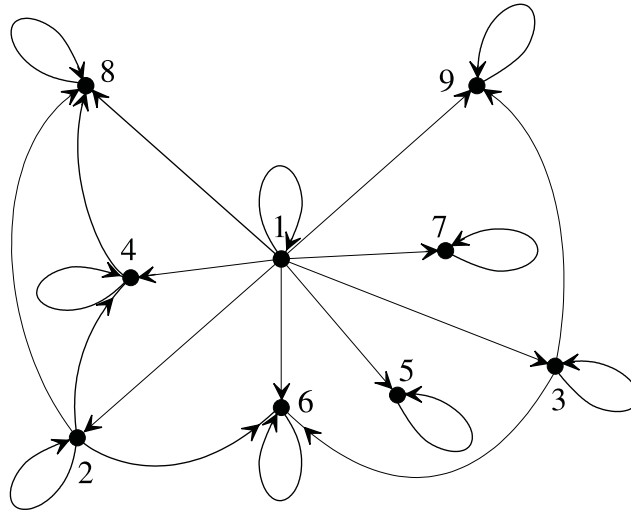
PRÍKLAD 1.38. Diagram orientovaného grafu z príkladu 1.37 je na obr. 2. ■

DEFINÍCIA 1.28. Ak hrana h orientovaného grafu G inciduje s dvoma rôznymi vrcholmi, nazýva sa **orientovaná linka** a ak inciduje len s jedným vrcholom, nazýva sa **orientovaná slučka**.

PRÍKLAD 1.39. V grafe G (obr. 2) hrany h_1, h_2, h_3, h_4, h_5 sú linky a hrana h_6 je slučka.

DEFINÍCIA 1.29. **Násobnosťou orientovanej hrany so začiatočným vrcholom u a koncovým vrcholom v** v orientovanom grafe G nazývame počet orientovaných hrán, ktorých začiatočný vrchol je u a koncový je v . Toto číslo budeme označovať $m(u, v)$.

Orientovaný graf nazývame **jednoduchý** (tiež **prostý**) **orientovaný graf**, ak pre každé dva jeho vrcholy u, v je $m(u, v) \leq 1$. Orientovaný graf, ktorý nie je jednoduchý sa nazýva **orientovaný multigraf**.



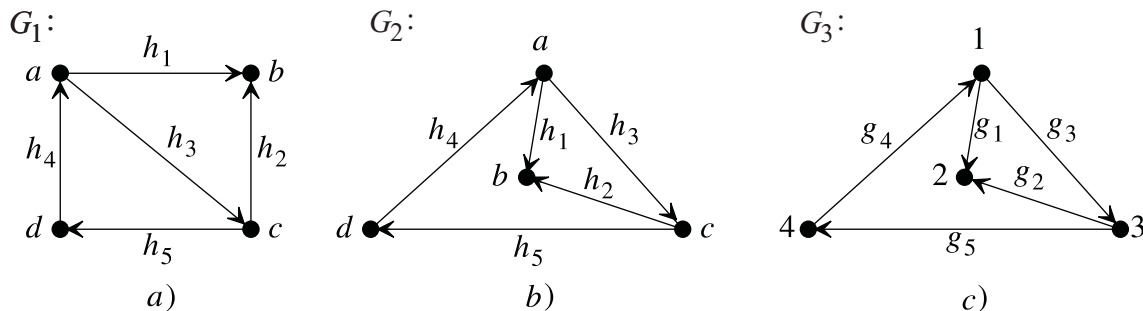
OBR. 3

Jednoduché grafy, presnejšie ich diagramy, nám umožňujú grafické znázornenie binárnych relácií na množine. Deje sa to takto:

Nech A je množina a $\sigma \subset A \times A$ je binárna relácia na množine A . Definujme graf $G = (A, \sigma, e)$, ktorého vrcholmi sú prvky množiny A , hranami sú usporiadané dvojice patriace do relácie σ a incidenciou je zobrazenie $e : \sigma \rightarrow A \times A$, $e(x, y) = (x, y)$. Graf $G = (A, \sigma, e)$ sa nazýva **orientovaný graf binárnej relácie σ** .

PRÍKLAD 1.40. Na množine $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ je definovaná relácia $\varrho = \{(x, y) \in A^2; x \mid y\}$. Orientovaný graf relácie ϱ (presnejšie jeho diagram) je na obr. 3. ■

Všimnime si diagramy grafov G_1, G_2 a G_3 na obr. 4. Grafy G_1 a G_2 sú rovnaké (majú rovnaké množiny vrcholov, množiny hrán a tiež incidencie). Grafy G_1 a G_3 sú rôzne. Ale keď porovnáme ich diagramy (G_1 na obr. 4a resp. 4b, lebo $G_1 = G_2$ a G_3 na obr. 4c),

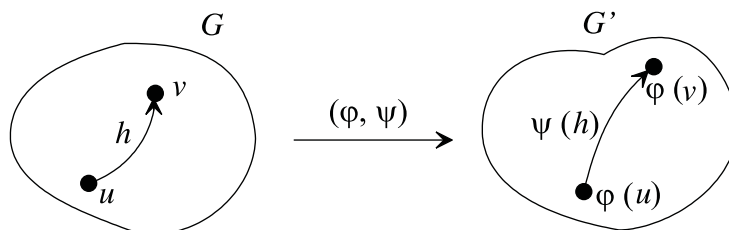


OBR. 4

vidíme, že medzi týmito grafmi nie je podstatný rozdiel, líšia sa iba v pomenovaní vrcholov a hrán. Takéto grafy budeme nazývať izomorfné.

Presná definícia je takáto:

DEFINÍCIA 1.30. Orientované grafy $G = (V, H, e), G' = (V', H', e')$ sa nazývajú **izomorfné**, ak existujú bijektívne zobrazenia $\varphi : V \rightarrow V', \psi : H \rightarrow H'$ také, že pre každú hranu $h \in H$ platí: ak $e(h) = (u, v)$, tak $e'(\psi(h)) = (\varphi(u), \varphi(v))$ (obr. 5).



OBR. 5

VETA 1.6. Nech $G = (V, H, e), G' = (V', H', e')$ sú jednoduché orientované grafy. Potom nasledujúce tvrdenia sú ekvivalentné:

- (a) G a G' sú izomorfné.
- (b) Existuje bijekcia $\varphi : V \rightarrow V'$ tak, že pre všetky $u, v \in V$ platí: u je začiatočný a v koncový vrchol jednej hrany práve vtedy, keď $\varphi(u)$ je začiatočný a $\varphi(v)$ koncový vrchol jednej hrany.

Dôkaz. Priamo z definície izomorfizmu grafov je zrejmé, že z (a) vyplýva (b). Dokážeme, že z (b) vyplýva (a). Nech teda $\varphi : V \rightarrow V'$ je bijekcia spĺňujúca podmienku: u je začiatočný a v koncový vrchol jednej hrany v grafe G práve vtedy, keď $\varphi(u)$ je začiatočný a $\varphi(v)$ koncový vrchol jednej hrany v grafe G' . Uvedená vlastnosť zobrazenia φ nám umožňuje definovať zobrazenie ψ medzi množinami hrán grafov G a G' týmto spôsobom:

$$\psi : H \rightarrow H', \psi(h) = h', \text{ pričom platí: ak } e(h) = (u, v), \text{ tak } e'(h') = (\varphi(u), \varphi(v))$$

Keďže φ je bijekcia a h je hrana v G práve vtedy, keď h' je hrana v G' , je ψ tiež bijekcia. $\square$

Predchádzajúcu vetu je možné zovšeobecniť aj pre multigrafy.

VERETA 1.7. Orientované grafy $G = (V, H, e)$, $G' = (V', H', e')$ sú izomorfné práve vtedy, keď existuje bijekcia $\varphi : V \rightarrow V'$ a pre každé vrcholy u, v orientovaného grafu G je $m(u, v) = m(\varphi(u), \varphi(v))$.

Dôkaz. Nech teda orientované grafy G a G' sú izomorfné. To znamená, že existujú také bijekcie $\varphi : V \rightarrow V'$, $\psi : H \rightarrow H'$, že pre každú hranu $h \in H$ platí: ak $e(h) = (x, y)$, tak $e'(\psi(h)) = (\varphi(x), \varphi(y))$. Nech $u, v \in V$ a $m(u, v) = k$. Ak $k = 0$, znamená to, že v grafe G neexistuje hrana so začiatočným vrcholom u a koncovým v . Potom ani v grafe G' neexistuje hrana so začiatočným vrcholom $\varphi(u)$ a koncovým $\varphi(v)$, v opačnom prípade by ψ nebola bijekcia. Ak $k \geq 1$, tak existuje k orientovaných hrán $h_1, \dots, h_k$, pre ktoré je

$$e(h_i) = (u, v), \quad i \in \{1, \dots, k\}.$$

Vzhľadom na to, že

$$e'(\psi(h_i)) = (\varphi(u), \varphi(v)), \quad \text{pre } i \in \{1, \dots, k\}$$

a ψ je bijekcia, je $m(\varphi(u), \varphi(v)) = k$.

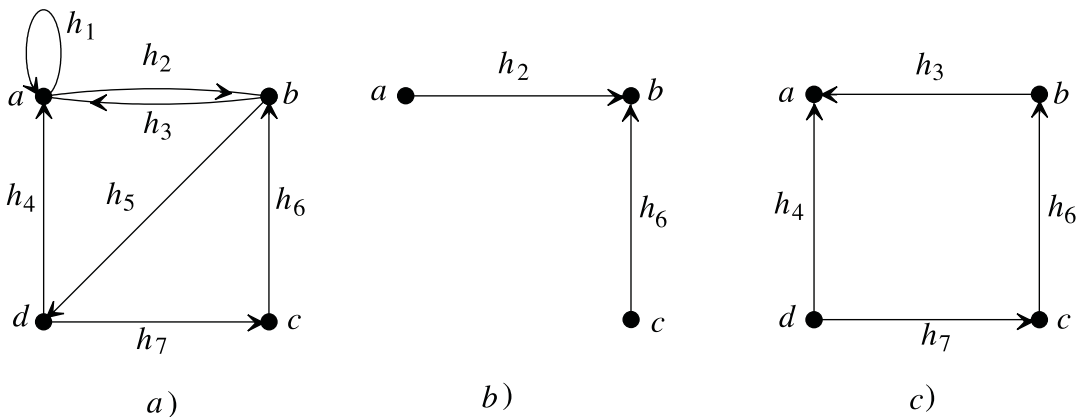
Dokážeme opačnú implikáciu. Nech teda existuje bijekcia $\varphi : V \rightarrow V'$ tak, že pre všetky $x, y \in V$ je $m(x, y) = m(\varphi(x), \varphi(y))$. Nech u je začiatočný a v koncový vrchol niektorej orientovanej hrany grafu G a nech $m(u, v) = k \geq 1$. Existuje teda práve k orientovaných hrán $h_1, \dots, h_k$ so začiatočným vrcholom u a koncovým v . Keďže $m(\varphi(u), \varphi(v)) = m(u, v)$, existuje v grafe G' k orientovaných hrán $g_1, \dots, g_k$ so začiatočným vrcholom $\varphi(u)$ a koncovým $\varphi(v)$. To nám umožňuje definovať zobrazenie ψ takto:

$$\psi : H \rightarrow H', \quad \psi(h_i) = g_i \quad \text{pre } i \in \{1, \dots, k\}.$$

Ľahko sa ukáže (prenechávame to čitateľovi), že ψ je bijektívne zobrazenie a že zobrazenia φ a ψ zachovávajú incidenciu. Grafy G a G' sú teda izomorfné. $\square$

DEFINÍCIA 1.31. Orientovaný graf $G' = (V', H', e')$ sa nazýva **podgraf** orientovaného grafu $G = (V, H, e)$, ak $V' \subset V$, $H' \subset H$, a e' je zúžením incidencie e na množinu hrán H' , t.j. pre každú hranu $h \in H'$ je $e'(h) = e(h)$.

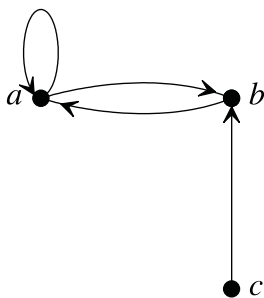
PRÍKLAD 1.41. Na obr. 6b, 6c sú podgrafy grafu G , ktorého diagram je na obr. 6a. $\blacksquare$



OBR. 6

DEFINÍCIA 1.32. Nech $G = (V, H, e)$ je orientovaný graf, $V' \subset V$, $V' \neq \emptyset$. Podgraf $G(V')$ orientovaného grafu G , ktorého množina vrcholov je V' a množina hrán H' je určená vlastnosťou: ak $u, v \in V'$, tak H' obsahuje všetky hrany z H , ktoré incidujú s oboma vrcholmi u, v , sa nazýva **indukovaný podgraf**.

PRÍKLAD 1.42. Nech G je graf z obr. 6a, $V' = \{a, b, c\}$. Indukovaný podgraf $G(V')$ grafu G je na obr. 7. ■



OBR. 7

DEFINÍCIA 1.33. Nech u, v sú vrcholy orientovaného grafu G , $k \in \mathbf{N}$. **Orientovaným sledom dĺžky k z vrchola u do vrchola v** nazývame postupnosť

$$v_0, h_1, v_1, h_2, v_2, \dots, v_{k-1}, h_k, v_k,$$

kde

1. $v_0, v_1, \dots, v_k$ sú vrcholy orientovaného grafu G ,
2. $h_1, \dots, h_k$ sú hrany orientovaného grafu G ,
3. pre $i \in \{1, \dots, k\}$ je v_{i-1} začiatkový a v_i koncový vrchol hrany h_i ,
4. $v_0 = u$, $v_k = v$.

Vrchol u sa nazýva **začiatočný** a vrchol v **koncový vrchol** tohto sledu.

PRÍKLAD 1.43. V grafe z obr. 6a je
 $a, h_1, a, h_2, b, h_5, d$ orientovaným sledom z vrcholu a do vrcholu d dĺžky 3,
 a, h_2, b, h_5, d orientovaným sledom z vrcholu a do vrcholu d dĺžky 2,
 a, h_1, a orientovaným sledom z vrcholu a do vrcholu a dĺžky 1,
 a orientovaným sledom z vrcholu a do vrcholu a dĺžky 0.

DEFINÍCIA 1.34. Orientovaný sled, v ktorom sa každá hrana grafu vyskytuje najviac raz, sa nazýva **orientovaný ťah**.

Orientovaný sled, v ktorom sa každý vrchol grafu vyskytuje najviac raz, sa nazýva **orientovaná cesta**.

DEFINÍCIA 1.35. Graf $G = (V, H, e)$ sa nazýva **silne súvislý** graf, ak pre každé dva vrcholy $u, v \in V$ existuje orientovaný sled z vrchola u do vrchola v .

DEFINÍCIA 1.36. Podgraf F grafu G sa nazýva **silne súvislý komponent** grafu G , ak platí:

1. F je indukovaný podgraf grafu G .
2. F je silne súvislý graf.
3. Ak $F' \neq F$ je taký podgraf grafu G , že F je jeho podgrafom, tak F' už nie je silne súvislý grafom.

V aplikáciách často k adekvátnemu opisu študovaného systému nestačí orientovaný graf, ale je potrebné k hranám a vrcholom pripísať nejaké údaje (najčastejšie číselné hodnoty). Graf, ktorého hrany a (alebo) vrcholy sú označené číselnými (alebo inými) hodnotami, sa nazýva ***ohodnotený graf***.