Algebraické štruktúry - Úvod
Binárna relácia a binárna operácia

Algebra a diskrétna matematika

Prednáška č. 9

doc. RNDr. Jana Šiagiová, PhD.

Priebežný test

29. 11. 2021 7:45 - 9:00 – učivo $1 - 8$ týždňa

Podmienka účasti na skúške je zisk minimálne 8 bodov z celkových 20.

Priebeh testu

- zápis na test do aisu najneskôr 23. 11. 2021 do 20:00
- napojenie na meeting o 7:45 pri zapnutej kamere (link mailom)
- identifikácia (celá tvár + identifikačná karta)
- odpísanie zadaní
- od 8:00 samostatné vypracovávanie na čistý papier (nie zošit) bez pozerania do obrazovky
- o 8:50 ukončenie vypracovávania
- odfotenie vašich riešení a vytvorenie pdf súboru (CamScanner)
- do 9:~~00~~ 05 odovzdanie pdf súboru do aisu
- na kamere musí byť počas celého priebehu testu vidieť vašu tvár, obidve ruky, papiere s riešeniami, ideálne celý stôl
- v miestnosti nemôže s vami byť nik iný
- stabilné internetové pripojenie
- nedodržanie niektorej z požiadaviek alebo akákoľvek forma podvodu budú hodnotené známkou FN bez možnosti účasti na skúške

Algebra ???

Poznáme zo strednej školy:

albegraický výraz

$$a^3 + 3, \quad \frac{x - y}{\sqrt{z} + \sqrt[3]{x}}, \quad \sqrt{3}p - q(r^6 + 9)$$

algebraická rovnica

$$x^2 - 4x + 5 = 0, \quad \pi\frac{a}{b} - 5 = a^5 + b$$

Elementárna algebra - zaoberá sa základnými vlastnosťami operácií na reálnych číslach, výrazmi a rovnicami, ktoré obsahujú reálne premenné

Moderná algebra = abstraktná algebra - náuka o abstraktných algebraických štruktúrach (zväz, grupa, pole a iné)

Aplikácie v teoretickej informatike:
kódovanie, šifrovanie, kvantová logika, analýza zložitosti algoritmov ...

Binárna relácia

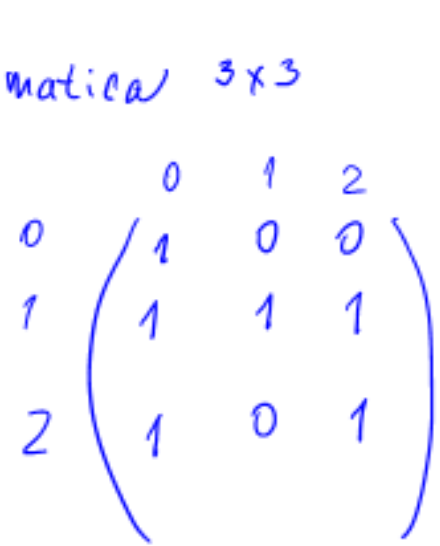
Nech M je neprázdna množina a nech $M \times M$ je **kartézsky súčin** množiny M samej so sebou, t.j. $M \times M = \{(x, y); x, y \in M\}$.

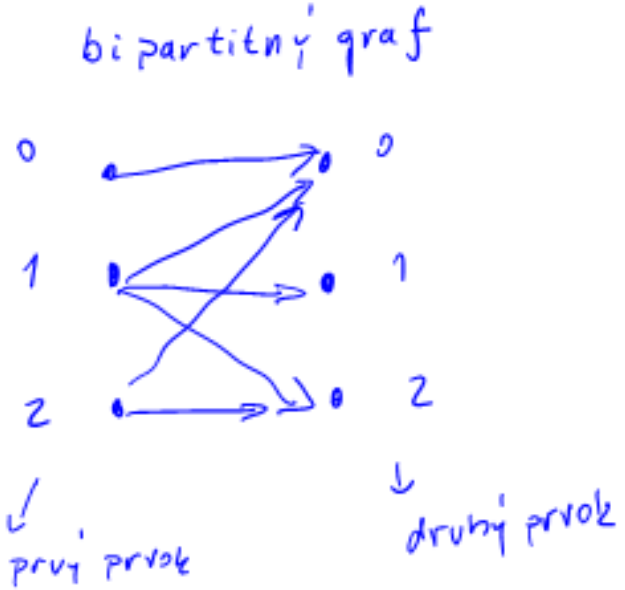
Pod **binárnou reláciou** na množine M rozumieme ľubovoľnú podmnožinu súčinu $M \times M$.

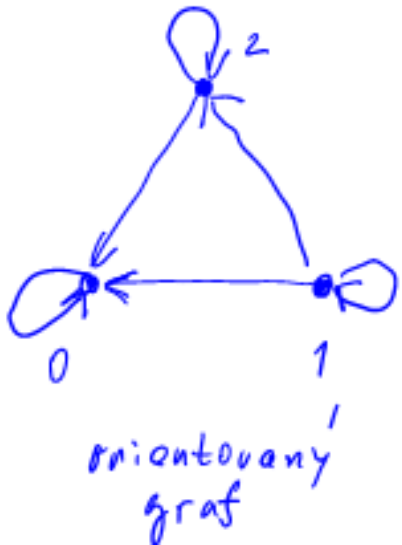
Formálne, $\mathcal{R}$ je binárna relácia na M, ak $\mathcal{R} \subseteq M \times M$.

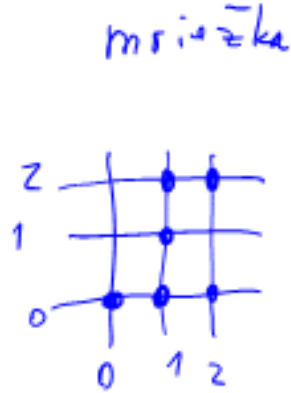
Vzťah medzi x a y v relácii $\mathcal{R}$ zapisujeme $(x, y) \in \mathcal{R}$ alebo $x\mathcal{R}y$.

Príklad 1: $M = \{0, 1, 2\}$, $\mathcal{R} = \{(0, 0), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2)\}$.







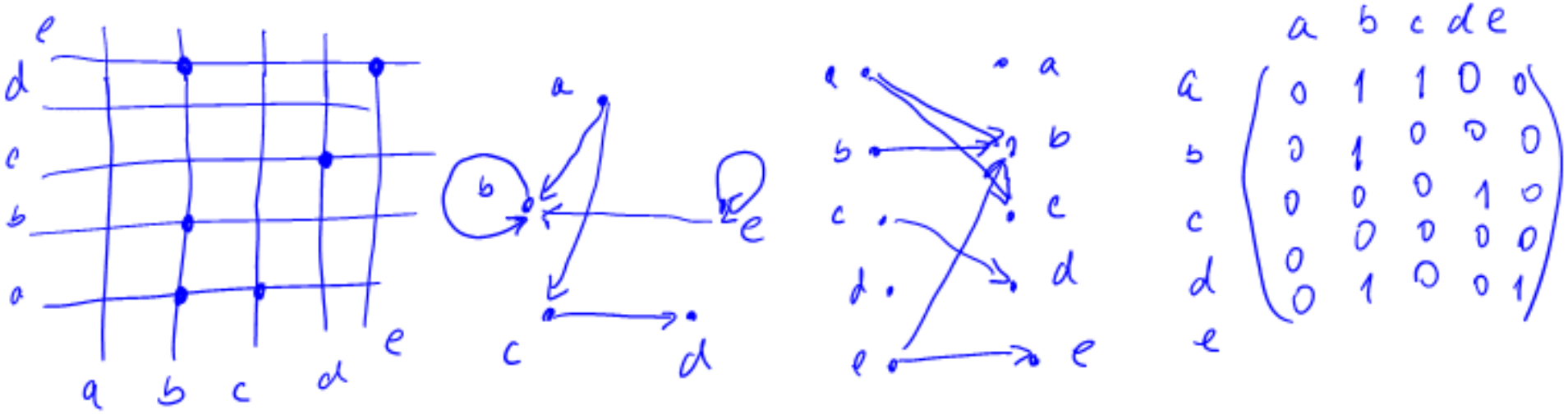


Binárna relácia - znázornenie

Ak $M = \{x_1, x_2, \ldots, x_n\}$, body v relácii $\mathcal{R}$ môžeme znázorniť pomocou

- **mriežky** $n \times n$ vyznačením zodpovedajúcich bodov
- **orientovaného grafu** s n vrcholmi, kde $x\mathcal{R}y$ je šípka z x do y
- **orientovaného bipartitného grafu** s $2n$ vrcholmi ($x\mathcal{R}y$: $x \to y$)
- **matice** $A_{n\times n} = (a_{ij})$, kde $a_{ij} = 1$, ak $x_i\mathcal{R}x_j$, inak $a_{ij} = 0$

Príklad 2: Na množine $M = \{a, b, c, d, e\}$ je daná binárna relácia $\mathcal{R} = \{(a, b), (a, c), (b, b), (c, d), (e, b), (e, e)\}$.



Binárna relácia a jej vlastnosti

Príklad 3: Na $M = \mathbb{Z}$ je binárna relácia $\mathcal{R} = \{(z, z+9); z \in \mathbb{Z}\}$.

Príklad 4: $\mathcal{R}$ na $\mathbb{R}$: $\quad x\mathcal{R}y \Leftrightarrow y = x^3 - x$

Poznámka: Funkcia je špeciálnym typom relácie.

Vlastnosti binárnej relácie

Hovoríme, že relácia $\mathcal{R}$ je na množine M

(R) **reflexívna**, ak pre každé $x \in M$ platí $x\mathcal{R}x$

(S) **symetrická**, ak $x\mathcal{R}y$ implikuje $y\mathcal{R}x$ pre každé $x, y \in M$

(A) **antisymetrická**, ak $x\mathcal{R}y$ a $y\mathcal{R}x$ implikuje $x = y$ pre každé $x, y \in M$

Binárna relácia a jej vlastnosti

Príklad 3: Na $M = \mathbb{Z}$ je binárna relácia $\mathcal{R} = \{(z, z+9); z \in \mathbb{Z}\}$.

Príklad 4: $\mathcal{R}$ na $\mathbb{R}$: $\quad x\mathcal{R}y \Leftrightarrow y = x^3 - x$

Poznámka: Funkcia je špeciálnym typom relácie.

Vlastnosti binárnej relácie

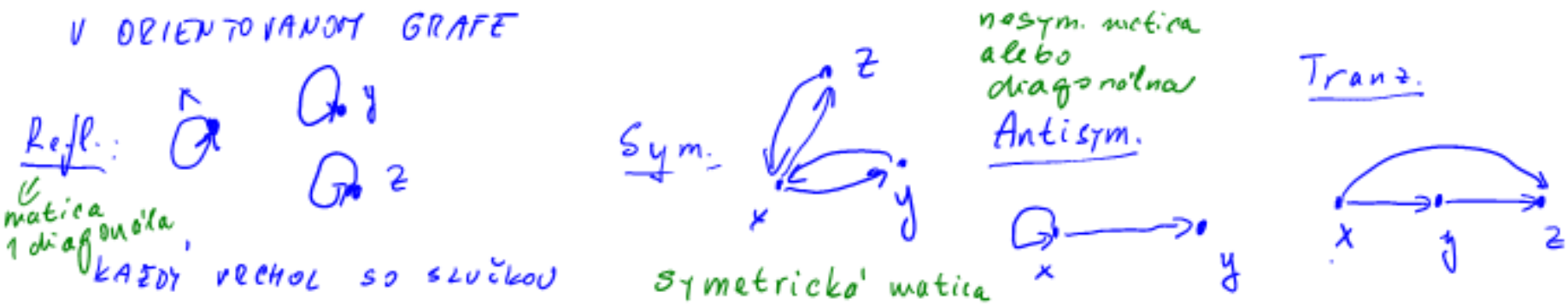
Hovoríme, že relácia $\mathcal{R}$ je na množine M

(R) **reflexívna**, ak pre každé $x \in M$ platí $x\mathcal{R}x$

(S) **symetrická**, ak $x\mathcal{R}y$ implikuje $y\mathcal{R}x$ pre každé $x, y \in M$

(A) **antisymetrická**, ak $x\mathcal{R}y$ a $y\mathcal{R}x$ implikuje $x = y$ pre každé $x, y \in M$

(T) **tranzitívna**, ak $x\mathcal{R}y$ a $y\mathcal{R}z$ implikuje $x\mathcal{R}z$ pre každé $x, y, z \in M$



Príklad

Príklad 5: Overte vlastnosti relácií na daných množinách

a) $M = \{0, 1, 2\}$, $\mathcal{R} = \{(0,0), (1,0), (1,1), (1,2), (2,0), (2,2)\}$

b) $\mathcal{R}$ na $\mathbb{R}$: $x\mathcal{R}y \Leftrightarrow |x - y| \geq 6$

a) reflex: $\forall x \in M: x \mathcal{R} x$ áno (0,0), (1,1), (2,2) ✓

sym. $\forall x, y \in M: x \mathcal{R} y \Rightarrow y \mathcal{R} x$ (1,0) ⇒ (0,1) nie — nie je sym.

antisym: $\forall x, y \in M: x \mathcal{R} y \wedge y \mathcal{R} x \Rightarrow x = y$

(1,0) nemá (0,1) ✓

(1,2) nemá (2,1) ✓

(2,0) nemá (0,2) ✓

je antisymetrická

tranzit. $\forall x, y, z \in M: x \mathcal{R} y \wedge y \mathcal{R} z \Rightarrow x \mathcal{R} z$

(1,0), 0...

(1,0), (0,0) ⇒ (1,0) ✓

(1,1) ∧ (1,2) ⇒ (1,2)

(2,0) ∧ (0,0) ⇒ (2,0)

(1,0) ∧ (0,0) ⇒ (1,0)

áno

b). Reflex: $\forall x \in R: |x - x| \geq 6 \rightarrow 0 \geq 6$ nie

Sym. $\forall x, y \in R: |x - y| \geq 6 \Rightarrow |y - x| \geq 6$ áno lebo $|x - y| = |y - x|$

Antisym. $\forall x, y \in R: |x - y| \geq 6 \wedge |y - x| \geq 6 \Rightarrow x = y$ nie pr. $x = 1$, $y = 7$

Tranz. $\forall x, y, z \in R: |x - y| \geq 6 \wedge |y - z| \geq 6 \Rightarrow |x - z| \geq 6$ $x = 7$, $y = 0$, $z = 7$

$|7 - 0| \geq 6 \wedge |0 - 7| \geq 6 \Rightarrow |7 - 7| \not\geq 6$ nie

Príklad

Príklad 6: Overte vlastnosti relácií na daných množinách

a) $\mathcal{R}$ na $\mathbb{Z}$: $x\mathcal{R}y \Leftrightarrow x \leq y$

b) M je množina všetkých priamok v rovine a $\mathcal{R}$ je relácia rovnobežnosti priamok, t. j. $\forall\, p, q \in M;\ p\mathcal{R}q \ \Leftrightarrow\ p \parallel q$

a). Reflex: $\forall x \in \mathbb{Z}: x \leq x$ áno

Sym: $\forall x, y \in \mathbb{Z}: x \leq y \Rightarrow y \leq x$ nie $x=1, y=2$, $1 \leq 2 \Rightarrow 2 \neq 1$

Antisym: $\forall x, y \in \mathbb{Z}: x \leq y \wedge y \leq x \Rightarrow x = y$ áno

$x \leq y \leq x \Rightarrow x = y$

Tranzit: $\forall x, y, z \in \mathbb{Z}: x \leq y$ a $y \leq z \overset{?}{\Rightarrow} x \leq z$ áno

$x \leq y \leq z \Rightarrow x \leq z$

b). Ref. $\forall p \in M: p \parallel p$ áno

Sym. $\forall p, q \in M: p \parallel q \Rightarrow q \parallel p$ áno (rovnaké smerové vektory)

Antisym. $\forall p, q \in M: p \parallel q \wedge q \parallel p \overset{?}{\Rightarrow} p = q$ nie

Tranzit. $\forall p, q, r \in M: p \parallel q \wedge q \parallel r \Rightarrow p \parallel r$ áno

Čiastočne usporiadaná množina (poset)

Binárna relácia $\mathcal{R} \subseteq M \times M$ sa nazýva **čiastočným usporiadaním** na M, ak je na M *reflexívna*, *antisymetrická* a *tranzitívna*.

Ak $\mathcal{R}$ je čiastočné usporiadanie na M, tak namiesto $x\mathcal{R}y$ používame označenie $x \preceq_{\mathcal{R}} y$ alebo sa index $\mathcal{R}$ vynecháva.
Často sa jednoducho píše $x \leq y$.

Vlastnosti z definície čiastočného usporiadania potom majú tvar

(R) $x \leq x$ (reflexívnosť)

(A) ak $x \leq y$ a $y \leq x$, tak $x = y$ (antisymetria)

(T) ak $x \leq y$ a $y \leq z$, tak $x \leq z$ (tranzitívnosť)

pre každé $x, y, z \in M$.

Dvojicu $(M, \leq)$, kde $\leq$ je binárna relácia čiastočného usporiadania, nazývame **čiastočne usporiadaná množina**.

ČUM

Príklad

Príklad 7: Nech S je neprázdna množina a nech M je ľubovoľná množina *podmnožín* množiny S. Nech $\leq$ je binárna relácia inklúzie, t.j. ak $X, Y \in M$, tak $X \leq Y$, ak X je podmnožinou množiny Y. Ukážte, že $(M, \leq)$ je čiastočne usporiadaná množina.

Ref. $\forall X, Y \in M: \quad X \subseteq X$ áno

Antisym. $\forall X, Y \in M: X \subseteq Y \wedge Y \subseteq X \Rightarrow X = Y$ áno

$X \subseteq Y: \forall a \in X \Rightarrow a \in Y$ a $X = Y$

$Y \subseteq X: \forall a \in Y \Rightarrow a \in X$

Tranz. $\forall X, Y, Z \in M: X \subseteq Y \wedge Y \subseteq Z \overset{?}{\Rightarrow} X \subseteq Z$

$\forall a \in X \Rightarrow a \in Y$

$\forall a \in Y \Rightarrow a \in Z$

$\Rightarrow \forall a \in X \Rightarrow a \in Z$

$X \subseteq Z$

Príklad

Príklad 8: Nech M je ľubovoľná neprázdna podmnožina množiny $\mathbb{N}$ a nech pre každé $x, y \in M$ symbol $x|y$ označuje fakt, že číslo x je deliteľom čísla y. Tvorí $(M, |)$ čiastočne usporiadanú množinu?

Reflex: $\forall x \in M : x \mid x$ áno

Antisym. $\forall x, y \in M : x \mid y \wedge y \mid x \Rightarrow x = y$ áno

$x \mid y$ $\quad \exists k \in N : y = kx \quad \Rightarrow y = kx = k\ell y$

$y \mid x$ $\quad \exists \ell \in N : x = \ell y$

$y = k\ell y \Rightarrow k \cdot \ell = 1$

$\Rightarrow k = 1 \wedge \ell = 1$

$\Rightarrow x = y$

Tranzitívnosť $\forall x, y, z \in M : x \mid y \wedge y \mid z \Rightarrow x \mid z$ áno

$\exists k \in N : y = kx$

$\exists \ell \in N : z = \ell y$

$z = \ell y = \underbrace{\ell k}_{m} x = mx$

$\exists m \in M : z = mx \Rightarrow x \mid z$

Porovnateľnosť prvkov

Ak $(M, \leq)$ je čiastočne usporiadaná množina, tak dva rôzne prvky $x, y \in M$ sú **porovnateľné**, ak buď $x \leq y$, alebo $y \leq x$.

(Oba vzťahy nemôžu platiť súčasne pre $x \neq y$.)

Budeme písať $x < y$, ak $x \leq y$ a $x \neq y$.

- Prvok $a \in M$ sa nazýva **najmenší**, ak $a \leq x$ pre každé $x \in M$.
- Prvok $b \in M$ sa nazýva **najväčší**, ak $x \leq b$ pre *každé* $x \in M$.
- Prvok $a \in M$ je **minimálny**, ak neexistuje žiadne $x \in M$, že $x < a$.
- Prvok $b \in M$ je **maximálny**, ak neexistuje žiadne $x \in M$, že $b < x$.

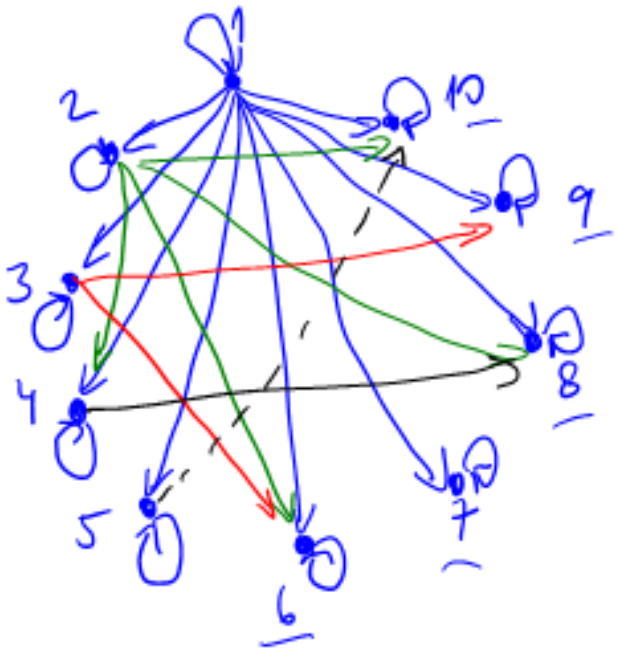
Ak v $(M, \leq)$ existuje najmenší (najväčší) prvok, tak tento je určený *jednoznačne*.

Najmenší (najväčší) prvok v $(M, \leq)$ je zároveň minimálnym (maximálnym) prvkom; vo všeobecnosti to neplatí obrátene.

Ak $(M, \leq)$ obsahuje viac ako jeden minimálny (maximálny) prvok, tak žiadne dva minimálne (maximálne) prvky nemôžu byť porovnateľné.

Binárna operácia

Príklad 9: Pre čiastočne usporiadanú množinu $(\{1, 2, \ldots, 10\}, |)$, kde $x \mid y$ označuje fakt, že x delí y, nájdite všetky minimálne a maximálne prvky, najmenší a najväčší prvok.



najmenší: 1 lebo
$\forall x \in M: 1 \mid x$

najväčší: 6 x 10 nexistuje
$\forall x \in M$

minimálny: 1

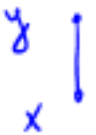
maximálny: 6, 7, 8, 9, 10
(nevychádza z nich hrana)

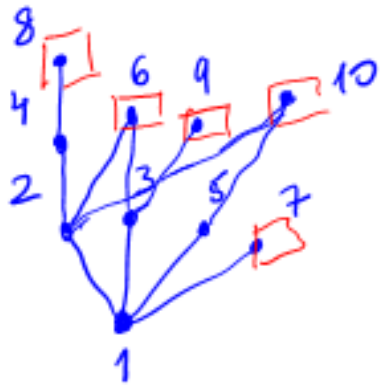
ČUM:

Ref. nepotr. ☺

TRANZ.

$x \leq y \rightarrow$





Hasseho diagram

Čiastočne usporiadané množiny znázorňuje pomocou **Hasseho diagramu**.

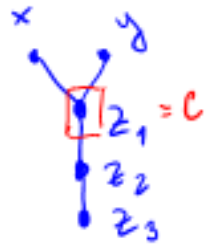
V Hasseho diagrame čiastočne usporiadanej množiny $(M, \leq)$:

- sa nevyskytujú slučky,
- spojnica je medzi x, y iba ak x je bezprostredným predchodcom prvku y, t.j. $x < y$ a neexistuje žiadne $z \in M$, že $x < z < y$,
- ak $x < y$, tak x sa umiestňuje pod y.

Z Haseho diagramu je možné jednoznačne zrekonštruovať reláciu $\leq$ čiastočného uporiadania na množine M.

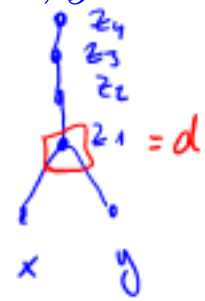
Zväzy

Nech $(M, \leq)$ je čiastočne usporiadaná množina a nech $x, y \in M$.



- Prvok $z \in M$ je **dolným ohraničením** prvkov x a y, ak $z \leq x$ a $z \leq y$.
- Prvok $c \in M$ je **najväčším dolným ohraničením** prvkov x a y, ak $c \leq x$, $c \leq y$, a ak $z \leq c$ pre každé dolné ohraničenie z prvkov x, y.

  Označenie: $c = \inf(x, y)$, alebo $c = x \wedge y$, *priesek* x a y.



- Prvok $z \in M$ je **horným ohraničením** prvkov x a y, ak $x \leq z$ a $y \leq z$.
- Prvok $d \in M$ je **najmenším horným ohraničením** prvkov x a y, ak $x \leq d$, $y \leq d$, a ak $d \leq z$ pre každé horné ohraničenie z prvkov x, y.

  Označenie: $d = \sup(x, y)$, alebo $d = x \vee y$, *spojenie* prvkov x a y.

Čiastočne usporiadaná množina $(M, \leq)$ sa nazýva **zväz**, ak pre každé $x, y \in M$ existuje ich priesek $x \wedge y$ a aj ich spojenie $x \vee y$.

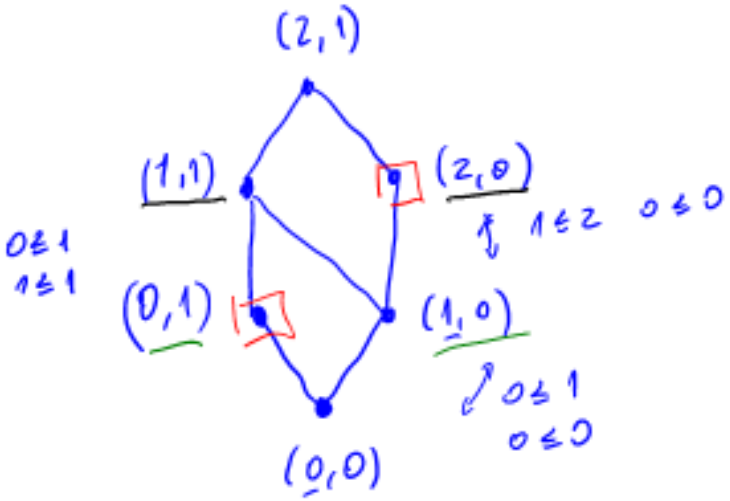
Príklad

Príklad 10: Nech $M = \{0,1,2\} \times \{0,1\}$ a relácia usporiadania $\leq$ je:

$(a,b) \overset{R}{\leq} (c,d) \Leftrightarrow a \leq c$ a $b \leq d$

$M = \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\}$

Rozhodnite, či $(M, \leq)$ tvorí zväz.



CHCEME UKÁZAŤ

$\forall x,y \in M \quad \exists x \wedge y \quad \exists x \vee y$

STAČÍ OVERIŤ PRE DVOJICE NEPORovnATEĽNÝCH PRVKOV

- DVOJICA $(0,1)$ a $(2,0)$

  $(0,1) \wedge (2,0) = (0,0)$ ✓

  $(0,1) \vee (2,0) = (2,1)$

- DVOJICA $(0,1)$ a $(1,0)$

  $(0,1) \wedge (1,0) = (0,0)$

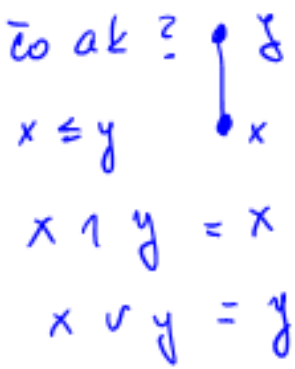
  $(0,1) \vee (1,0) = (1,1)$

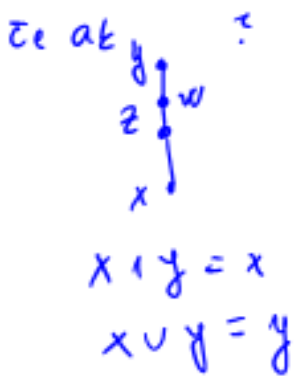
- DVOJICA $(1,1)$ a $(2,0)$

  $(1,1) \wedge (2,0) = (1,0)$

  $(1,1) \vee (2,0) = (2,1)$

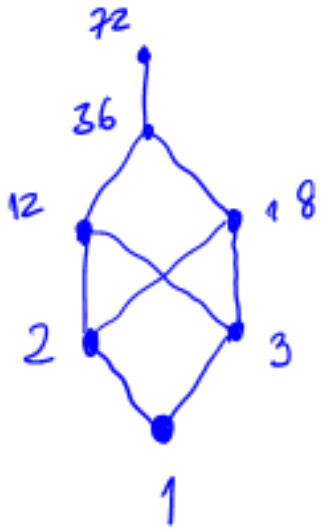
a'no je to zväz





Príklad

Príklad 11: Na množine $M = \{1, 2, 3, 12, 18, 36, 72\}$ uvažujeme binárnu reláciu deliteľnosti $|$. Rozhodnite, či $(M, |)$ je zväz.



NETOROVN. PRVKY

2, 3

$2 \wedge 3 = 1$

$2 \vee 3$ = určka sa 12 aj 18 ⇒ neexistuje

horná ohraničenie 2 a 3 : 12, 18, 36, 72

$12 \nmid 18$

lebo $12 \nmid 18$

$12 \vee 18 = 36$

$12 \wedge 18$ neexistuje

nie je zväz

Príklady

Príklad 12: Nech $(\mathbb{N}, |)$ je čiastočne usporiadaná množina, kde $\mathbb{N}$ je množina prirodzených čísiel a $x \mid y$ označuje fakt, že x delí y. Potom $x \wedge y$ je najväčší spoločný deliteľ a $x \vee y$ je najmenší spoločný násobok čísiel x a y; čiastočne usporiadaná množina$(\mathbb{N}, |)$ je zväz.

Príklad 13: Nech S je neprázdna množina a nech 2^S označuje množinu *všetkých* podmnožín množiny S. V čiastočne usporiadanej množine $(2^S, \subseteq)$ je priesek dvoch prvkov rovný prieniku a spojenie je rovné zjednoteniu príslušných množín a teda $(2^S, \subseteq)$ je zväz.

Takéto zväzy sa nazývajú **boolovské**.

Lineárne usporiadanie

Čiastočne usporiadaná množina $(M, \leq)$ sa nazýva **reťazec**, ak pre každé $x, y \in M$ platí, že $x \leq y$ alebo $y \leq x$;
skrátene, ak každé dva prvky v M sú *porovnateľné*.

Príslušné čiastočné usporiadanie $\leq$ sa nazýva aj **lineárne**.

Tvrdenie: Každý reťazec je zväz.

Príklad 14: Overte či dané čiastočné usporiadané množiny sú reťazce.
a) $(\{1, 2, 3, 4, 5, 6\}, \leq)$
b) $M = \{1, 2, 3, 4\}$, $\mathcal{R} = \{(2, 3), (2, 1), (1, 4), (1, 3), (2, 4), (4, 3)\}$