

# Matematická logika

## Relace a algebry (13.přednáška)



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání  
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

# Obsah

- Množiny (opakování)
- Relace a zobrazení (opakování)
  - Relace
  - Binární relace na množině
  - Zobrazení
  - Rozklady, ekvivalence
  - Uspořádání
- Algebry
  - Algebry s jednou operací
  - Algebry se dvěma operacemi
  - Svazy

# Teorie množin

- **Jazyk:**

- *Speciální symboly:*

- *Binární predikáty:*  $\in$  (je prvkem),  $\subset$  (je vlastní podmnožinou),  $\subseteq$  (je podmnožinou).
    - *Binární funkční symboly:*  $\cap$  (průnik),  $\cup$  (sjednocení).

- **Cantor** – naivní teorie (bez axiomatizace).

- Dnes – poměrně mnoho formálních axiomatizací – žádná z nich *není úplná*.

- *Příklady:* *von Neumann-Bernays-Gödel, Zermelo-Fränkel + axiom výběru.*



# Zermelo-Fränkel set- theory

**Axiom of extensionality:** Two sets are the same if and only if they have the same elements.

**Axiom of empty set:** There is a set with no elements.

**Axiom of pairing:** If  $x, y$  are sets, then so is  $\{x, y\}$ , a set containing  $x$  and  $y$  as its only elements.

**Axiom of union:** Every set has a **union**. That is, for any set  $x$  there is a set  $y$  whose elements are precisely the elements of the elements of  $x$ .

**Axiom of infinity:** There exists a set  $x$  such that  $\{\}$  is in  $x$  and whenever  $y$  is in  $x$ , so is the union  $y \cup \{y\}$ .

**Axiom of separation** (or subset axiom): Given any set and any **proposition**  $P(x)$ , there is a **subset** of the original set containing precisely those elements  $x$  for which  $P(x)$  holds.

**Axiom of replacement:** Given any set and any **mapping**, formally defined as a proposition  $P(x, y)$  where  $P(x, y)$  and  $P(x, z)$  implies  $y = z$ , there is a set containing precisely the images of the original set's elements.

**Axiom of power set:** Every set has a **power set**. That is, for any set  $x$  there exists a set  $y$ , such that the elements of  $y$  are precisely the subsets of  $x$ .

**Axiom of regularity** (or *axiom of foundation*): *Every non-empty set  $x$  contains some element  $y$  such that  $x$  and  $y$  are disjoint sets.*

**Axiom of choice:** *(Zermelo's version) Given a set  $x$  of mutually disjoint nonempty sets, there is a set  $y$  (a choice set for  $x$ ) containing exactly one element from each member of  $x$ .*

# Množiny

- $\emptyset$  - prázdná množina
- Počet prvků množiny  $A$ :  $|A|$

## Vztahy mezi množinami (*axiomy*):

- Rovnost

$A = B$  právě když  $(\forall x : x \in A \Leftrightarrow x \in B)$

- Inkluze

$A \subseteq B$  právě když  $(\forall x : x \in A \Rightarrow x \in B)$



# Množiny – množinové operace

- Průnik

$$A \cap B = \{x; x \in A \text{ a } x \in B\}$$

- Sjednocení

$$A \cup B = \{x; x \in A \text{ nebo } x \in B\}$$

- Rozdíl

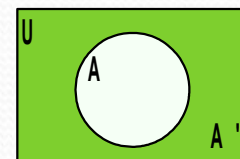
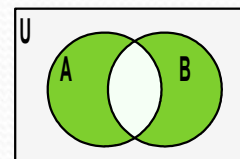
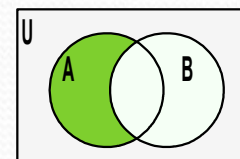
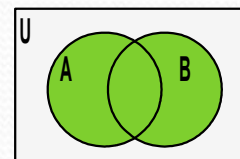
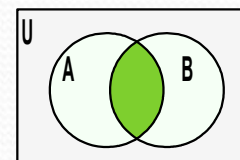
$$A - B = \{x; x \in A \text{ a } x \notin B\}$$

- Symetrický rozdíl

$$A \oplus B = (A \cup B) - (A \cap B)$$

- Doplněk vzhledem k univerzu U

$$A' = U - A$$



# Množiny – množinové operace

- Potenční množina

$$2^A = \{X; X \subseteq A\}$$

- Kartézský součin

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

- Kartézská mocnina

$$A^n = \underbrace{A \times A \times \cdots \times A}_n$$

$$A^1 = A, A^0 = \{\emptyset\}$$



# Relace

- $n$ -ární relace mezi množinami  $A_1, A_2, \dots, A_n$

$$r \subseteq A_1 \times A_2 \times \dots \times A_n$$

- *Příklad:*

- $D$  = množina možných dnů
- $M$  = množina místností VŠB
- $Z$  = množina zaměstnanců VŠB

Ternární relace *schůze* (kdy, kde, kdo):  
 $r \subseteq D \times M \times Z$



# Binární relace

$$r \subseteq A \times B$$

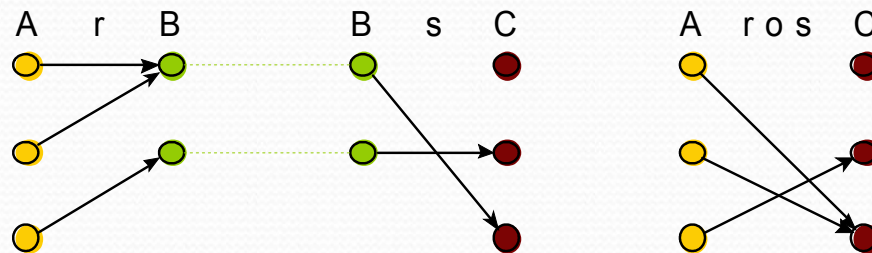
- Inverzí relace k  $r$ :

$$r^{-1} = \{(x, y) \in B \times A : (y, x) \in r\}$$

- Složení (kompozice) relací

$$r \subseteq A \times B, s \subseteq B \times C$$

$$r \circ s = \{(x, y) \in A \times C : (\exists z \in B) ((x, z) \in r \text{ a } (z, y) \in s)\}$$



# Binární relace

Binární relace  $r$  na množina  $A$  je:

- *Reflexivní*:  $\forall x \in A: (x,x) \in r$
- *Ireflexivní*:  $\forall x \in A: (x,x) \notin r$
- *Symetrická*:  $\forall x,y \in A: (x,y) \in r \Rightarrow (y,x) \in r$
- *Antisymetrická*:  $\forall x,y \in A: (x,y) \in r \text{ a } (y,x) \in r \Rightarrow x=y$
- *Asymetrická*:  $\forall x,y \in A: (x,y) \in r \Rightarrow (y,x) \notin r$
- *Tranzitivní*:  $\forall x,y,z \in A: (x,y) \in r \text{ a } (y,z) \in r \Rightarrow (x,z) \in r$
- *Cyklická*:  $\forall x,y,z \in A: (x,y) \in r \text{ a } (y,z) \in r \Rightarrow (z,x) \in r$
- *Souvislá*:  $\forall x,y \in A: x=y$  nebo  $(x,y) \in r$  nebo  $(y,x) \in r$



# Binární relace

## Důležité typy binárních relací:

- Tolerance – reflexivní, symetrická
- Kvaziuspořádání – reflexivní, tranzitivní
- Ekvivalence – reflexivní, symetrická, tranzitivní
- (částečné neostré) uspořádání – reflexivní, antisymetrická, tranzitivní



# Binární relace

Příklady:

- Tolerance:
  - „být podobný“ na množině lidí,
  - „mít odlišný věk nejvýše o jeden rok“ na množině lidí, ...
- Kvaziuspořádání:
  - „množiny  $X$  a  $Y$  jsou v relaci, pokud  $|X| \leq |Y|$ “ na množině množin,
  - relace dělitelnosti na množině celých čísel,
  - „nebýt starší“ na množině lidí, ...
- Ekvivalence:
  - „být stejně starý“ na množině lidí,
  - rovnost na množině přirozených čísel, ...
- Uspořádání:
  - relace inkluze,
  - relace dělitelnosti na množině přirozených čísel, ...

# Zobrazení (funkce)

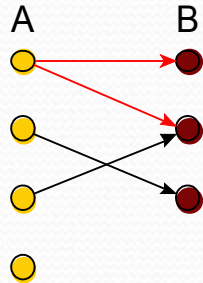
- $f \subseteq A \times B$  se nazývá **zobrazení Z množiny A do množiny B** (parciální zobrazení), jestliže platí:  
 $(\forall x \in A, \forall y_1, y_2 \in B) ( (x, y_1) \in f \text{ a } (x, y_2) \in f \Rightarrow y_1 = y_2 )$
- $f$  se nazývá **zobrazení množiny A do množiny B** (totální zobrazení, značíme  **$f: A \rightarrow B$** ), jestli platí:
  - $f$  je zobrazení z  $A$  do  $B$
  - $(\forall x \in A)(\exists y \in B) ( (x, y) \in f )$
- Je-li  $f$  zobrazení,  $(x, y) \in f$  píšeme jako  **$f(x)=y$**



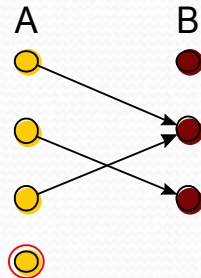
# Zobrazení (funkce)

- *Příklady:*

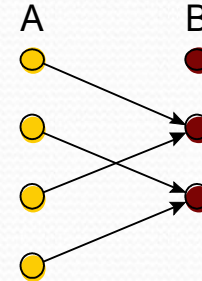
$r \subseteq A \times B$



$s \subseteq A \times B$



$t \subseteq A \times B$



$$u = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}; x = y^2\},$$

$$v = \{(x, y) \in \mathbb{N} \times \mathbb{N}; x = y^2\},$$

$$w = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}; y = x^2\}$$

- $r, u$  - nejsou zobrazení
- $s, v$  - parciální zobrazení z  $A$  do  $B$ , není totální
- $t, w$  - totální zobrazení



# Zobrazení (funkce)

Zobrazení  $f: A \rightarrow B$  se nazývá:

- **Injektivní** (*prosté*), platí-li:

$$\forall x_1, x_2 \in A, \forall y \in B: (x_1, y) \in f \text{ a } (x_2, y) \in f \Rightarrow x_1 = x_2$$

- **Surjektivní** (*zobrazení na*), platí-li:

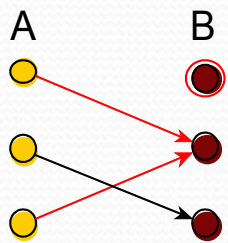
$$\forall y \in B \exists x \in A: (x, y) \in f$$

- **Bijektivní** (*vzájemně jednoznačné*), je-li současně *injektivní* i *surjektivní*.

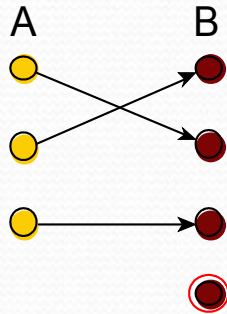
# Zobrazení (funkce)

- Příklady

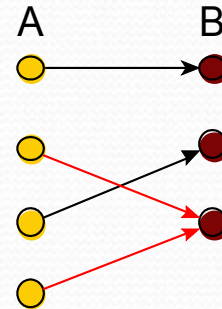
$f : A \rightarrow B$



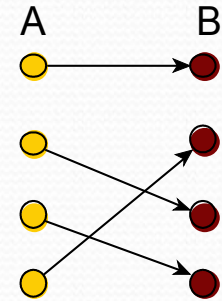
$g : A \rightarrow B$



$h : A \rightarrow B$



$i : A \rightarrow B$



$j: \mathbb{Z} \rightarrow \mathbb{Z}, j(n) = n^2, \quad k: \mathbb{Z} \rightarrow \mathbb{N}, k(n) = |n|,$   
 $l: \mathbb{N} \rightarrow \mathbb{N}, l(n) = n + 1, m: \mathbb{R} \rightarrow \mathbb{R}, j(x) = x^3$

- $f, j$  - nejsou *injektivní* ani *surjektivní*
- $h, k$  - jsou *surjektivní*, nejsou *injektivní*
- $g, l$  - jsou *injektivní*, nejsou *surjektivní*
- $l, m$  - jsou *injektivní* i *surjektivní*  $\Rightarrow$  *bijekce*

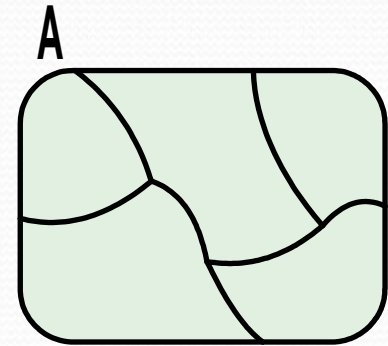


# Rozklady a ekvivalence

- Rozklad na množině  $A$  je systém:

$X = \{ X_i; i \in I \}$  takový že:

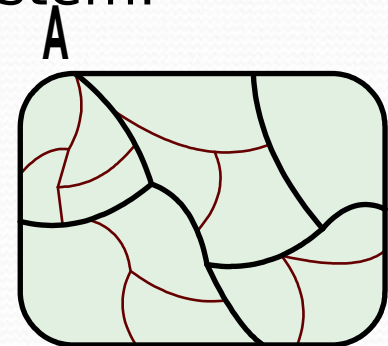
- $X_i \subseteq A$  pro  $\forall i \in I$
- $X_i \cap X_j = \emptyset$  pro  $\forall i, j \in I, i \neq j$
- $\bigcup X = A$   
 $X_i$  - třídy rozkladu



- Zjemněním rozkladu  $X = \{ X_i; i \in I \}$  je systém:

$Y = \{ Y_j; j \in J \}$ , jestliže:

- $\forall j \in J, \exists i \in I$  takové, že  $Y_j \subseteq X_i$





# Rozklady a ekvivalence

- Necht'  $r$  je relace ekvivalence na množině  $A$ ,  $X$  je rozklad na  $A$ , pak:
  - $X_r = \{[x]_r; x \in A\}$  - rozklad na  $A$  (*rozklad indukovaný ekvivalencí  $r$ , faktorová množina množiny  $A$  podle ekvivalence  $r$* ).
  - $r_X = \{(x,y); x \text{ a } y \text{ patří do stejné třídy rozkladu } X\}$  - ekvivalence na  $A$  (*indukovaná rozkladem  $X$* ).

*Příklad:*

- $r \subseteq \mathbb{Z} \times \mathbb{Z}; \quad r = \{(x,y); 3 \text{ dělí } x-y\} \quad \Rightarrow \quad X = \{X_1, X_2, X_3\}$
- $X_1 = \{\dots -6, -3, 0, 3, 6, \dots\}$
- $X_2 = \{\dots -5, -2, 1, 4, 7, \dots\}$
- $X_3 = \{\dots -4, -1, 2, 5, 8, \dots\}$

# Uspořádání

- Je-li  $r$  relace uspořádání na  $A$ , pak se dvojice  $(A, r)$  nazývá **uspořádaná množina**.

- Značení  $(A, \leq)$

- *Příklady:*  $(\mathbb{N}, \leq)$ ,  $(2^M, \subseteq)$

- Relace pokrytí

Nechť  $(A, \leq)$  uspořádaná množina,  $(a, b) \in A$

$a \prec b$  („ $b$  pokrývá  $a$ “) jestliže

$a < b$  a  $\neg \exists c \in A: a \leq c$  a  $c \leq b$

- *Příklad:*  $(\mathbb{N}, \leq)$ ,  $\prec = \{(n, n+1); n \in \mathbb{N}\}$



# Uspořádání

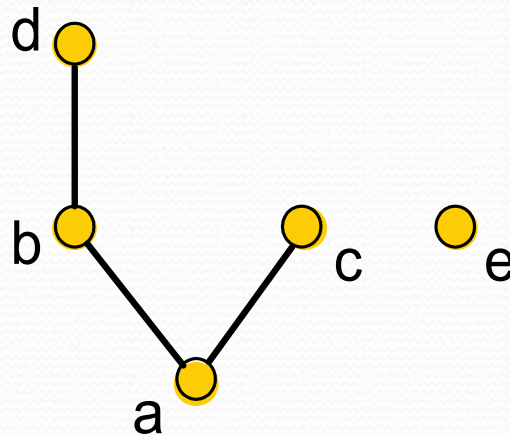
- Hasseovy diagramy – grafické znázornění

- *Příklad:*

$(A, \leq)$ ,  $A = \{a, b, c, d, e\}$

$r = \{(a, b), (a, c), (a, d), (b, d)\} \cup id_A$

$id_A = \{(a, a) : a \in A\}$



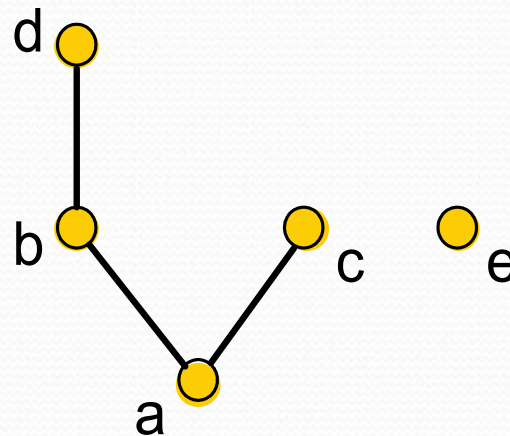
# Uspořádání

Prvek  $a$  uspořádané množiny  $(A, \leq)$  se nazývá:

- **Nejmenší:** pro  $\forall x \in A: a \leq x$
- **Největší:** pro  $\forall x \in A: x \leq a$
- **Minimální:** pro  $\forall x \in A: (x \leq a \Rightarrow x = a)$
- **Maximální:** pro  $\forall x \in A: (a \leq x \Rightarrow x = a)$

- **Příklad:**

- Nejmenší: *neexistuje*
- Největší: *neexistuje*
- Minimální:  $a, e$
- Maximální:  $d, c, e$





# Uspořádání

- Uspořádané množiny  $(A, \leq)$ ,  $(B, \leq)$  se nazývají **izomorfní**, existuje-li bijekce  $f: A \rightarrow B$  tak, že:

$$\forall x, y \in A: x \leq y \text{ právě když } f(x) \leq f(y)$$

- Jsou-li  $(A, \leq)$ ,  $(B, \leq)$  uspořádané množiny, nazývají se zobrazení  $f: A \rightarrow B$  **izotonní**, platí-li:

$$\forall x, y \in A: x \leq y \Rightarrow f(x) \leq f(y)$$

- **Příklad:**

- $f: \mathbb{N} \rightarrow \mathbb{Z}$ ,  $f(x) = kx$ ,  $k \in \mathbb{Z}$ ,  $k \geq 0$  je izotonní
- $g: \mathbb{N} \rightarrow \mathbb{Z}$ ,  $g(x) = kx$ ,  $k \in \mathbb{Z}$ ,  $k \leq 0$  není izotonní

# Uspořádání

- Necht'  $(A, \leq)$  uspořádaná množina,  $M \subseteq A$ , pak
- $L_A(M) = \{x \in A; \forall m \in M: x \leq m\}$ 
  - Množina dolních závor (dolní kužel)
- $U_A(M) = \{x \in A; \forall m \in M: m \leq x\}$ 
  - Množina horních závor (horní kužel)
- $\text{Inf}_A(M)$  – největší prvek množiny  $L_A(M)$ 
  - Infimum množiny  $M$
- $\text{Sup}_A(M)$  – nejmenší prvek množiny  $U_A(M)$ 
  - Supremum množiny  $M$



# Svaz - svazově uspořádaná množina

- Množina  $(A, \leq)$  se nazývá **svaz** (svazově uspořádaná množina), platí-li:

$$\forall x, y \in A \quad \exists s, i \in A : s = \sup(\{x, y\}), i = \inf(\{x, y\})$$

- Značení:
  - $x \vee y = \sup(\{x, y\})$
  - $x \wedge y = \inf(\{x, y\})$
- Existuje-li  $\sup(M)$  a  $\inf(M)$  pro **každou**  $M \subseteq A$ , nazývá se  $(A, \leq)$  **úplný svaz**.

# Algebry

**Algebra** (*univerzální algebra*) je dvojice:  **$(A, F^A)$** :

- $A \neq \emptyset$  - nosič algebry
  - $F^A = \{f_i: A^{p(f_i)} \rightarrow A; i \in I\}$  - množina operací na  $A$
  - $p(f_i)$  - arita operace  $f_i$
- *Příklady:*
- $(\mathbb{N}, +, \cdot)$   
*množina přirozených čísel s operacemi sčítání a násobení*
  - $(2^M, \cap, \cup)$   
*množina všech podmnožin množiny  $M$  s operacemi průnik a sjednocení*
  - $(F, \vee, \wedge)$   
*množina  $(F)$  formulí výrokové logiky s operacemi konjunkce a disjunkce*



# Algebry s jednou binární operací

Grupoid  $\mathbf{G}=(G,\bullet)$

- $\bullet: G \times G \rightarrow G$
- Je-li množina  $G$  konečná, grupoid  $\mathbf{G}$  se nazývá **konečný**.
- Řád grupoidu =  $|G|$

*Příklady grupodů:*

- $G_1=(\mathbb{R}, +)$ ,  $G_2=(\mathbb{R}, \cdot)$ ,  $G_3=(\mathbb{N}, +)$  ...

# Algebry s jednou binární operací

- Konečný grupoid  $\mathbf{G}=(G,\bullet)$  lze popisovat pomocí *Cayleyovy tabulky*.

- *Příklad*:  $G = \{a,b,c\}$

$\bullet$	$a$	$b$	$c$
$a$	$a$	$b$	$c$
$b$	$a$	$c$	$c$
$c$	$a$	$a$	$b$

- Např.:  $a \bullet b = b$ ,  $b \bullet a = a$ ,  $c \bullet c = b \dots$



# Algebry s jednou binární operací

Nechť  $\mathbf{G}=(G, \bullet)$  je grupoid  $\mathbf{G}$  se nazývá:

- Komutativní, platí-li v  $\mathbf{G}$ :
  - $(\forall a, b \in G)(a \bullet b = b \bullet a)$
- Asociativní, platí-li v  $\mathbf{G}$ :
  - $(\forall a, b, c \in G)((a \bullet b) \bullet c = a \bullet (b \bullet c))$
- S jednotkovým (neutrálním) prvkem, platí-li v  $\mathbf{G}$ :
  - $(\exists e \in G \forall a \in G)(a \bullet e = a = e \bullet a)$
- S nulovým (agresivním) prvkem, platí-li v  $\mathbf{G}$ :
  - $(\exists o \in G \forall a \in G)(a \bullet o = o = o \bullet a)$
- S inverzními prvky, platí-li v  $\mathbf{G}$ :
  - $(\forall a \in G \exists b \in G)(a \bullet b = e = b \bullet a)$

# Algebry s jednou binární operací

*Příklady:*

- $(R, \cdot), (N, +)$  – komutativní i asociativní.
- $(R, \bullet), a \bullet b = (a+b) / 2$  – komutativní, není asociativní.
- $(R, \bullet), a \bullet b = a^b$  – není komutativní ani asociativní.
- $(R, \cdot)$  –  $1 =$  jednotkový prvek,  $0 =$  nulový prvek.



# Algebry s jednou binární operací

Nechť  $\mathbf{G}=(G, \bullet^G)$  je grupoid.  $H \subseteq G$  se nazývá **uzavřená** (vzhledem k operaci  $\bullet^G$ ), platí-li:

- $(\forall a, b \in H)(a \bullet^G b \in H)$

Grupoid  $\mathbf{H}=(H, \bullet^H)$  je **podgrupoidem** grupoidu  $\mathbf{G}=(G, \bullet^G)$ , platí-li:

- $\emptyset \neq H \subseteq G$  je uzavřená
- $\forall a, b \in H: a \bullet^H b = a \bullet^G b$

- *Příklady:*

- $(\mathbb{N}, +^{\mathbb{N}})$  je podgrupoidem  $(\mathbb{Z}, +^{\mathbb{Z}})$
- $\{0, 1, 2\}$  není nosičem podgrupoidu  $(\mathbb{Z}, +^{\mathbb{Z}})$

# Algebry s jednou binární operací

- Nechť  $\mathbf{G}_1=(G_1, \bullet^1)$ ,  $\mathbf{G}_2=(G_2, \bullet^2)$ .
- $\mathbf{G}_1 \times \mathbf{G}_2=(G_1 \times G_2, \bullet)$  – **direktní součin  $\mathbf{G}_1$  a  $\mathbf{G}_2$** , kde:
  - $(a_1, a_2) \bullet (b_1, b_2) = (a_1 \bullet^1 b_1, a_2 \bullet^2 b_2)$

*Příklad:*

- $\mathbf{G}_1=(Z, +)$ ,  $\mathbf{G}_2=(Z, \cdot)$ .
- $\mathbf{G}_1 \times \mathbf{G}_2=(Z \times Z, \bullet)$ ,
- $(a_1, a_2) \bullet (b_1, b_2) = (a_1 + b_1, a_2 \cdot b_2)$
- $(1,2)(3,4) = (1+3, 2 \cdot 4) = (4,8)$  atd.



# Algebry s jednou binární operací

- Nechť  $\mathbf{G} = (G, \bullet_{\mathbf{G}})$ ,  $\mathbf{H} = (H, \bullet_{\mathbf{H}})$  jsou grupoidy a  $h: G \rightarrow H$  zobrazení.
- $h$  se nazývá **homomorfismus** grupoidu  $\mathbf{G}$  do grupoidu  $\mathbf{H}$ , platí-li:
- $\forall a, b \in G: h(a \bullet_{\mathbf{G}} b) = h(a) \bullet_{\mathbf{H}} h(b)$

Typy homomorfismů:

- **Monomorfismus** -  $h$  je injektivní
- **Epimorfismus** -  $h$  je surjektivní
- **Izomorfismus** -  $h$  je bijektivní
- **Endomorfismus** -  $\mathbf{H} = \mathbf{G}$
- **Automorfismus** - bijektivní a  $\mathbf{H} = \mathbf{G}$

# Algebry s jednou binární operací

$r$  je **kongruence** na grupoidu  $\mathbf{G}=(G, \bullet_{\mathbf{G}})$ , pokud:

- $r$  je binární relace:  $\theta \subseteq G \times G$
- $r$  je ekvivalence
- $(a_1, a_2), (b_1, b_2) \in r \Rightarrow (a_1 \bullet_{\mathbf{G}} b_1, a_2 \bullet_{\mathbf{G}} b_2) \in r$

**faktorový grupoid** grupoidu  $\mathbf{G}$  podle kongruence  $r$ :

$$\mathbf{G}/r=(G/r, \bullet_{\mathbf{G}/r}), [a]_r \bullet_{\mathbf{G}/r} [b]_r = [a \bullet_{\mathbf{G}} b]_r$$

*Příklad:*

- $r \subseteq \mathbb{Z} \times \mathbb{Z}; \quad r = \{(x,y); 3 \text{ dělí } x-y\}$
- $r$  je kongruence na  $(\mathbb{Z}, +)$

	$\bullet$	[0]	[1]	[2]
[0]		[0]	[1]	[2]
[1]		[1]	[2]	[0]
[2]		[2]	[0]	[1]



# Algebry s jednou binární operací

Typy grupoidů:

- **Pologrupa** - asociativní grupoid.
- **Monoid** - pologrupa s jednotkovým prvkem.
- **Grupa** - monoid s inverzními prvky.
- **Abelova grupa** - komutativní grupa.

*Příklady:*

- $(\mathbb{Z}, -)$  - grupoid, není pologrupou
- $(\mathbb{N} - \{0\}, +)$  - pologrupa, není monoidem.
- $(\mathbb{N}, \cdot)$  - monoid, není grupou.
- $(\mathbb{Z}, +)$  - Abelova grupa.

# Algebry se dvěma binárními operacemi

Algebra  $(A, +, \cdot)$  se nazývá **Okruh**, platí-li:

- $(A, +)$  je komutativní grupa
- $(A, \cdot)$  je monoid
- pro  $\forall a, b, c \in A$  platí:  $a \cdot (b + c) = a \cdot b + a \cdot c$ ,  $(b + c) \cdot a = b \cdot a + c \cdot a$
- Je-li  $|A| > 1$ , nazývá se  $(A, +, \cdot)$  **netriviální okruh**.
- Nechť  $\mathbf{0} \in A$  je neutrální prvek grupy  $(A, +)$ . Pak  $\mathbf{0}$  se nazývá **nulou okruhu**  $(A, +, \cdot)$ .
- Nechť  $\mathbf{1} \in A$  je jednotkový prvek monoidu  $(A, \cdot)$ . Pak  $\mathbf{1}$  se nazývá **jednotkou (jedničkou) okruhu**  $(A, +, \cdot)$ .



# Algebry se dvěma binárními operacemi

Okruh  $(A, +, \cdot)$  se nazývá **těleso**, platí-li:

- $(A - \{0\}, \cdot)$  je komutativní grupa

*Příklady:*

- $(\mathbf{Z}, +, \cdot)$  – okruh, není těleso
- $(\mathbf{R}, +, \cdot)$ ,  $(\mathbf{C}, +, \cdot)$  – tělesa

# Svaz – algebraická struktura

- Svaz  $L = (L, \vee, \wedge)$
- $\vee: L \times L \rightarrow L, \quad \wedge: L \times L \rightarrow L$
- $\forall x, y, z \in L$  platí:

$x \vee x = x$	$x \wedge x = x$	idempotence
$x \vee y = y \vee x$	$x \wedge y = y \wedge x$	komutativita
$x \vee (y \vee z) = (x \vee y) \vee z$	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$	asociativita
$x \vee (x \wedge y) = x$	$x \wedge (x \vee y) = x$	absorpce



# Svaz – algebraická struktura

Nechť  $(A, \vee, \wedge)$  je svaz,  $(B, \leq)$  je svazově uspořádaná množina:

- Definujme na  $A$  relaci  $\leq_v$ :

$$a \leq_v b \text{ právě když } a \vee b = b$$

- Definujme na  $B$  operace  $\vee_{\leq}$  a  $\wedge_{\leq}$

$$a \vee_{\leq} b = \sup\{a, b\}, \quad a \wedge_{\leq} b = \inf\{a, b\},$$

Pak platí:

- $(A, \leq)$  je svazově uspořádaná množina, kde:

$$\sup\{a, b\} = a \vee b, \quad \inf\{a, b\} = a \wedge b$$

- $(B, \vee_{\leq}, \wedge_{\leq})$  je svaz
- $(A, \vee, \wedge) = (A, \vee_{\leq}, \wedge_{\leq})$

# Svaz – algebraická struktura

Svaz  $(L, \wedge, \vee)$  je

- **Modulární**, platí-li  $\forall x, y, z \in L$  :

$$x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$$

- **Distributivní**, platí-li  $\forall x, y, z \in L$  :

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

- **Komplementární**, platí-li:

Existuje nejmenší prvek  $0 \in L$ , největší prvek  $1 \in L$

$$\forall x \in L \exists x' \in L : x \wedge x' = 0, x \vee x' = 1$$

$x'$  se nazývá **doplňkem** (komplementem) prvku  $x$

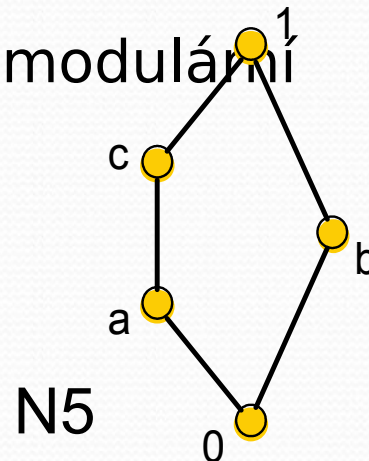
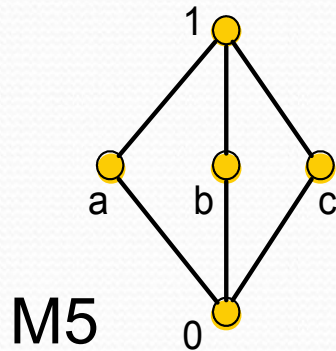


# Svaz – algebraická struktura

- Každý distributivní svaz je modulární

*Příklad:*

- M5 (*diamant*) – modulární svaz, který není distributivní
- N5 (*pětiúhelník*) – není modulární



# Svaz – algebraická struktura

Svaz  $(L, \vee, \wedge)$  se nazývá **Booleův svaz**, je-li:

- Komplementární, distributivní s nejmenším prvkem  $0 \in L$  a největším prvkem  $1 \in L$

**Booleova algebra:**

- $(L, \vee, \wedge, -, 0, 1)$ ,  $- : L \rightarrow L$  je operace komplementu v  $L$

*Příklad:*

- $(2^A, \cup, \cap)$ ,  $A = \{1, 2, 3, 4, 5, 6, 7\}$

